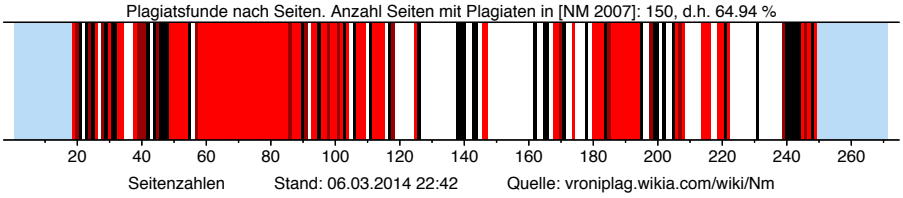
Report: Nm

From VroniPlag Wiki

This report is based on the findings of an on-going plagiarism analysis (date: 2014-03-06). It is therefore not a final or conclusive report. It is recommended to visit the page http://de.vroniplag.wikia.com/wiki/Nm for the current state of the findings and further information.

A critical discussion of the thesis by Prof. Dr. Nasrullah Memon: Investigative Data Mining: Mathematical Models for Analyzing, Visualizing and Destabilizing Terrorist Networks

Submitted to the Department of Computer Science and Engineering (http://www.cs.aau.dk/en/) of the Esbjerg Institute of Technology (http://www.en.esbjerg.aau.dk/) at Aalborg Universitet Esbjerg (http://www.esbjerg.aau.dk/) in partial fulfillment of the requirements for the degree of Doctor of Philosophy. Thesis committee: Prof. Dr. Henrik Legind Larsen (http://vbn.aau.dk/en/persons/henrik-legind-larsen%28b686118d-6daf-4022-840f-846762685da7%29.html) , Prof. Dr. Hsinchun Chen (http://mis.eller.arizona.edu/faculty/hchen.asp) , Prof. Dr. Jørgen Fischer Nilsson (http://www2.imm.dtu.dk/~jfn/) , Prof. Dr. Kim Bæhr Larsen. Published: 2007. → ISBN 978-87-7606-020-6.



The barcode displays a visualization of the pages that contain plagiarism, not the amount of plagiarism in the main text. Depending on the amount of plagiarized text there are three colors that are used:

- black: up to 50 % of the lines on the page are plagiarized
- dark red: between 50 % and 75 % of the lines on the page are plagiarized
- light red: over 75 % of the lines on the page are plagiarized.

White pages have either not yet been investigated or nothing was found. Blue pages contain matter such as the title page, the table of contents, the reference section, empty pages and appendices. These are all not included in the calculations.

The barcode only shows the current state of the investigation. This is not the final result, as each case may continue to be worked on and added to by anyone as new sources turn up. Thus, a final state does not exist.

There are **150** pages containing plagiarism.

Pages with less than 50% plagiarism

43 pages: 021 023 025 029 031 032 042 044 046 047 048 055 090 095 103 106 111 117 126 138 139 140 143 144 162 165 166 171 178 184 195 199 200 202 205 221 231 240 241 242 243 244 248

Pages with between 50%-75% plagiarism

19 pages: 020 024 028 039 040 041 045 057 086 091 098 101 118 170 185 198 207 239 246

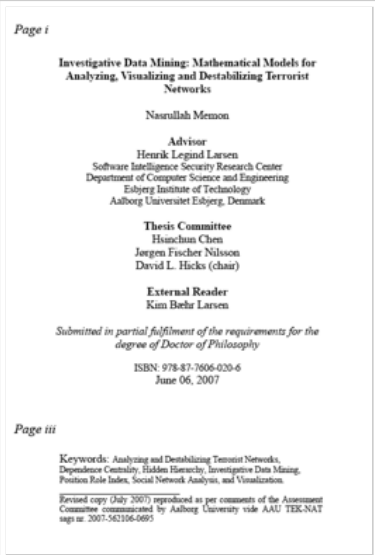
Pages with more than 75% plagiarism

88 pages: 019 026 030 033 034 038 049 050 051 052 053 054 058 059 060 061 062 063 064 065 066 067 068 069 070 071 072 073 074 075 076 077 078 079 080 081 082 083 084 085 087 088 089 093 094 096 097 099 100 102 104 107 108 109 112 113 114 115 125 146 147 168 169 174 180 181 182 183 186 187 188 189 190 191 192 193 194 206 208 214 215 216 219 220 222 245 247 249

Thesis Version

The PhD thesis of Nasrullah Memon analysed in the VroniPlag Wiki has the following characteristics:

- Title: Investigative Data Mining: Mathematical Models for Analyzing, Visualizing and Destabilizing Terrorist Networks
- 271 pages
- Year of publication: 2007
- ISBN: 978-87-7606-020-6
- Submitted at the Department of Computer Science and Engineering (http://www.cs.aau.dk/en/) , Esbjerg Institute of Technology (http://www.en.esbjerg.aau.dk/) at Aalborg Universitet Esbjerg (http://www.esbjerg.aau.dk/)
- Advisor: Prof. Dr. Henrik Legind Larsen (http://vbn.aau.dk/en/persons/henrik-legind-larsen%28b686118d-6daf-4022-840f-846762685da7%29.html)
- Thesis Committee: Prof. Dr. Hsinchun Chen (http://mis.eller.arizona.edu/faculty/hchen.asp) , Prof. Dr. Jørgen Fischer Nilsson (http://www2.imm.dtu.dk/~jfn/) , Prof. Dr. David L. Hicks (http://personprofil.aau.dk/110432) (chair)
- External Reader: Prof. Dr. Kim Bæhr Larsen



Page i

Investigative Data Mining: Mathematical Models for Analyzing, Visualizing and Destabilizing Terrorist Networks

Nasrullah Memon

Advisor
Henrik Legind Larsen
Software Intelligence Security Research Center
Department of Computer Science and Engineering
Esbjerg Institute of Technology
Aalborg Universitet Esbjerg, Denmark

Thesis Committee
Hsinchun Chen
Jørgen Fischer Nilsson
David L. Hicks (chair)

External Reader
Kim Bæhr Larsen

Submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

ISBN: 978-87-7606-020-6
June 06, 2007

Page iii

Keywords: Analyzing and Destabilizing Terrorist Networks, Dependence Centrality, Hidden Hierarchy, Investigative Data Mining, Position Role Index, Social Network Analysis, and Visualization.

Revised copy (July 2007) reproduced as per comments of the Assessment Committee communicated by Aalborg University vide AAU TEK-NAT sags nr. 2007-562106-0695

Title Pages of the thesis analysed in the Vroniplag Wiki

As reported by the Danish press (e.g. [1] (http://www.information.dk/telegram/299951) , [2] (http://www.b.dk/nationalt/terrorforsker-mistaenkes-for-omfattende-snyd) or [3] (http://nyhederne.tv2.dk/article.php/id-50105993:forsker-mist%C3%A6nkt-for-fusk-med-afhandling.html?rss&ss)), N. Memon seems to claim that he was exposed to a plot, and the thesis analysed in the VroniPlag Wiki was not the same thesis he has submitted for examination and revised in 2007. While VroniPlag Wiki naturally cannot provide ultimate proof that the thesis analysed is in fact the same as the thesis originally submitted by N. Memon, there is convincing evidence that there was no such plot and the real thesis was analysed:

- The PDF file analysed in the VroniPlag Wiki was created in December 2007 according to file properties and available for download from Memon's SDU website until 2011 according to an anonymous informant. The same version of the thesis was sent to the VroniPlag Wiki by two individuals separately.
- Many of the publications Memon has (co-)authored before as well as after the submission of the thesis contain text that can be found identically or almost identically in the version of Memon's thesis that has been analysed in the VroniPlag Wiki. This includes about half of the text that has been identified as plagiarism in Memon's thesis (see here). For an overview of Memon's publications other than the PhD thesis that contain copied text, see here.
  - eight of those publications have already been retracted by the publisher (see here), many more contain text that originally was not written by the authors and might be retracted in the future.
- Memon cites his own thesis in many of his (co-)authored publications (see here (http://scholar.google.de/scholar?cites=10839406331418069858&as_sdt=2005&sciodt=0,5&hl=en)). Sometimes he even cites his PhD thesis for text that he has copied into his PhD thesis from unreferenced sources (for a detailed overview, see this table of quotations).

Prominent findings

- Almost four pages of the thesis (79 (first half), 80, 81, 82) are copied from the paper Xu et al. (2004) with only minor adjustments and without mentioning this paper anywhere in the thesis. A member of the thesis committee (Hsinchun Chen) is one of the co-authors of this paper, which leads to the question, why he did not notice the plagiarism when he read the thesis.
  - Other papers (co-)authored by Chen are also among the not sufficiently referenced sources: Xu & Chen (2003), Chen (2006), Xu & Chen (2005a), Xu & Chen (2005b)
- The pages 192, 193, 194, and 195 are taken from the publication Smith & King (2002). This is interesting, because a paper written in 2009 (after the dissertation) by four authors, Nm and the chair of the thesis committee D.L. Hicks among them, has been retracted by the IEEE, because it contained non-attributed original text from the same source, see the retraction notice. (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5066528&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5066528)
- In many instances the copied text is adapted to make it more suitable for the terrorist theme of the thesis, often subsituting the word "terrorists" for "criminals". Some examples are given here:
  - Nm/Fragment_194_01
  - Nm/Fragment_019_01
- Several pages of the thesis are copied from the "Military Guide to Terrorism in the Twenty-First Century". This publication is mentioned in the thesis in two places, but not in the bibliography. The copied text typically has been adapted only slightly. On page 64 a figure has been copied from the Military Guide without reference.
- The dissertation of Hamill (2006) is the source for parts of the "Problem Definition", the "Research Objectives" and the "Conclusions and Recommendations" sections. Even the final words of the thesis are plagiarised: Nm/Fragment_249_01. The first sentences of the thesis are also copied (but from another source): Nm/Fragment_019_01
- Nm/Fragment_026_04: not only has an entire paragraph been taken literally from Koschade (2005). It is then attributed to Memon & Larsen (2006), while references that can be found in the original source have been removed. The same copied text is used twice in the thesis, see also: Nm/Fragment_045_18
- Nm/Fragment 104 12: Two equations and explaining text have been copied from Koschuetzki et al. (2005). At most places index names have been changed from *s* and *t* (source) to *u* and *w* (thesis), but in one instance *s* and *t* remain in the thesis, which makes no mathematical sense but shows the original source of the paragraph.
- Nm/Fragment_206_01: Even the description of structural aspects of the knowledge-base that constitutes the empirical core of the thesis is a literal copy from a publication that is nowhere mentioned in the thesis: Zhao et al. (2006) This leads to the question to what degree this knowledge-base is an original creation of Nm.

Other observations

- In this thesis one finds text copied from a large number of sources (see Quelle:Nm). The amount of text copied from each individual source, however, tends not to be very large. Most of the time the source is not mentioned anywhere close to the borrowed text, and often the source is not mentioned anywhere in the thesis at all.
- Several chapter and section titles are commented with a footnote indicating that the entire following section is taken from another publication. This might be acceptable when the author mentions -- as he does several times in the thesis -- that he has published the material previously himself. But how should one interpret the following footnotes on chapter titels?
  - FN 9 (page 49): *Some parts of this Sections are taken from "A Military Guide to Terrorism in 21st Century"* [note: this Military Guide is not listed in the bibliography]
  - FN 14 (page 95): *Most of the concepts discussed in this section are taken from West B. Douglas (2001).*
  - FN 19 (page 125): *The most of the text is taken from http://en.wikipedia.org/...*
  - FN 20 (page 130): *The most of the text for this section is taken from http://www.globalsecurity.org/... (http://www.globalsecurity.org/security/profiles/uss_cole_bombing.htm) http://en.wikipedia.org/...*
  - FN 31 (page 183): *The matter is taken from (Heer et al., 2005)* [note: Heer et al. 2005 is not listed in the bibliography]
- There are several references to the Wikipedia, without specifying which date the Wikipedia article has been consulted (footnotes on pages 121, 125, 130, 166, 170, 171)
- Several text fragments appear in the thesis more than once, for example:
  - Page 19 and page 93 are almost identical. The parallel text continues on page 20-21 and 94-95 respectively. However, on the latter pages slight changes have been made. See for instance: Nm/Fragment_019_01 and Nm/Fragment_093_04.
  - A shorter paragraph can be found three times in the thesis and once in another publication from where it probably has been copied. See Nm/Fragment_091_11, Nm/Fragment_033_15 und Nm/Fragment_040_22.
  - Also used twice: Nm/Fragment_045_18 and Nm/Fragment_026_04
- Large parts of the thesis have been published elsewhere, either before or after the publication of the thesis. Not surprisingly these other publications "inherit" fragments of copied text. Some examples are listed here, a more comprehensive overview can be found here. In fact, about half of all fragments documented in the thesis of Nm can be found also in other publications, see here.
- Nm often states in the thesis that a certain section or chapter has been published previously elsewhere. However, there are also various examples where thesis material has been previously published somewhere else without this being mentioned in the thesis. While these instances of self-plagiarism are beyond the scope of the present documentation, one example is listed here:
  - Pages 223-226 of the thesis are taken from Memon & Larsen (2006c) (http://books.google.es/books?id=jausP_1AGU8C&pg=PA1043&lpg=PA1043&dq=%22variation+seen+in+the+participation+index+we+conclude+that%22&source=bl&ots=X2YiaZEqG6&sig=w1V9jPPGgCnSHcTpvM6tR8xEPpE&hl=en&sa=X&ei=4kyeT8ytMoOt0QXa0eX2Dg&redir_esc=y#v=onepage&q=%22variation%20seen%20in%20the%20participation%20index%20we%20conclude%20that%22&f=false)

Statistic

- Currently there are 227 reviewed fragments documented that are considered to be plagiarism. For 201 of them there is no reference given to the source used („Verschleierungen" and „Komplettplagiate"). For 26 fragments the source is given, but the extent of the used text is not made clear („Bauernopfer").
- The publication has 231 pages that have been analyzed. On a total of 150 of these pages plagiarism has been documented. This represents a percentage of **64.9%**. The 231 analyzed pages break down with respect to the amount of plagiarism encountered as follows:

Percentage plagiarism	Number of pages
No plagiarism documented	81
0%-50% Plagiarism	43
50%-75% Plagiarism	19
75%-100% Plagiarism	88

  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 37%** of the main part of the publication.

- In all, text was taken from 64 sources.

Illustration

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

- grau="Komplettplagiat" (copy & paste): the source of the text parallel is not given, the copy is verbatim.
- rot="Verschleierung" (disguised plagiarism): the source of the text parallel is not given, the copied text will be somewhat modified.
- gelb="Bauernopfer" (pawn sacrifice): the source of the text parallel is mentioned, but the extent and/or the closeness of the copy to the source is not made clear by the reference.

Definitions of plagiarism categories

The plagiarism categories used here are based on the discussion found at Wohnsdorf / Weber-Wulff: Strategien der Plagiatsbekämpfung, 2006 (http://www.htw-berlin.de/organisation/?typo3state=publications&lsfid=1274) . A complete description of the categories (in German) can be found at the VroniPlag-Wiki. In particular, the categories are:

Komplettplagiat (copy and paste)

The source of the text parallel is not given, the copy is verbatim.

Verschleierung (disguised plagiarism)

The source of the text parallel is not given, the copied text will be somewhat modified or disguised.

Bauernopfer (pawn sacrifice)

The source of the text parallel is mentioned, but the extent and/or closeness of the copying is not made clear by the reference.

Sources tabulated by plagiarism category

The following table lists all of the **reviewed** fragments by source (rows) and by plagiarism category (columns).

- ÜP = Translation plagiarism,
- KP = Copy and paste,
- VS = Disguised plagiarism,
- BO = Pawn sacrifice,
- KW = No opinion,
- KeinP = Not plagiarism.

Table: Nm: Sources / Fragments

Source	Year	ÜP	KP	VS	BO	KW	KeinP	∑	To be reviewed	In progress Nm
Arquilla Ronfeldt	2001	0	1	7	0	0	0	**8**	**0**	**0**
Aviv et al	2003	0	1	1	0	0	0	**2**	**0**	**0**
Balasundaram et al	2006	0	1	4	0	0	0	**5**	**0**	**0**
Bedi	2005	0	0	1	2	0	0	**3**	**0**	**0**
Berry etal	2004	0	0	2	0	0	0	**2**	**0**	**0**
Borgatti	2002	0	2	3	0	0	0	**5**	**0**	**0**
Brandes Erlebach	2005	0	1	2	0	0	0	**3**	**0**	**0**
CNS	2002	0	1	4	0	0	0	**5**	**0**	**0**
Carley	2006	0	0	2	0	0	0	**2**	**0**	**0**
Chen	2006	0	0	5	0	0	0	**5**	**0**	**0**
Clark etal	2005	0	0	1	0	0	0	**1**	**0**	**0**
Clauset Young	2005	0	0	1	0	0	0	**1**	**0**	**0**
Combating Terrorism Center	2006	0	0	1	1	0	0	**2**	**0**	**0**
DCSINT	2005	0	1	18	2	0	0	**21**	**0**	**0**
DeRosa	2004	0	0	0	6	0	0	**6**	**0**	**0**
Dombroski Carley	2002	0	0	2	0	0	0	**2**	**0**	**0**
Dugan etal	2006	0	0	2	0	0	0	**2**	**0**	**0**
Freeman	1980	0	0	3	0	0	0	**3**	**0**	**0**
Frost	1982	0	1	1	1	0	0	**3**	**0**	**0**
Hamill	2006	0	0	10	0	1	0	**11**	**0**	**0**
Han Kamber	2006	0	0	2	0	0	0	**2**	**0**	**0**
Heer et al	2005	0	0	10	1	0	0	**11**	**0**	**0**
Holmgren	2006	0	3	0	0	0	0	**3**	**0**	**0**
Jensen et al	2003	0	2	0	0	0	0	**2**	**0**	**0**
Katz et al	2004	0	0	3	1	0	0	**4**	**0**	**0**
Koelle et al	2006	0	2	1	0	0	0	**3**	**0**	**0**
Koschade	2005	0	1	2	0	0	0	**3**	**0**	**0**
Koschuetzki etal	2005	0	1	2	0	0	0	**3**	**0**	**0**
Krebs	2002	0	0	1	0	0	0	**1**	**0**	**0**
Krebs	2004	0	0	0	2	0	0	**2**	**0**	**0**
Latora and Marchiori	2004	0	0	1	1	0	0	**2**	**0**	**0**
Lemieux	2003	0	0	4	0	0	0	**4**	**0**	**0**
Malin etal	2005	0	0	1	0	0	0	**1**	**0**	**0**
Padhy	2006	0	0	0	0	0	0	**0**	**1**	**0**
Penzar etal	2005	0	0	4	0	0	0	**4**	**0**	**0**
Perer Shneiderman	2006	0	0	6	0	0	0	**6**	**0**	**0**
Popp and Poindexter	2006	0	0	1	0	0	0	**1**	**0**	**0**
Qin et al	2005	0	0	0	1	0	0	**1**	**0**	**0**
Ressler	2006	0	2	9	1	0	0	**12**	**0**	**0**
Saxena et al.	2004	0	0	3	0	0	0	**3**	**0**	**0**
Scott	1987	0	0	2	0	0	0	**2**	**0**	**0**
Shelley	2002	0	2	3	2	0	0	**7**	**0**	**0**
Shelley Picarelli	2002	0	0	0	0	3	0	**3**	**0**	**0**
Smith and King	2002	0	0	4	0	0	0	**4**	**0**	**0**
Stephenson and Zelen	1989	0	3	3	0	0	0	**6**	**0**	**0**
Stokman	2004	0	0	2	0	0	0	**2**	**0**	**0**
The Dark Web Project	2010	0	0	0	0	0	0	**0**	**1**	**0**
TrackingTheThreat.com	2006	0	1	2	0	0	0	**3**	**0**	**0**
TrackingTheThreat.com	2006a	0	0	1	0	0	0	**1**	**0**	**0**

Source	Year	ÜP	KP	VS	BO	KW	KeinP	∑	To be reviewed	In progress Nm
Tsvetovat et al.	2005	0	0	2	0	0	0	**2**	**0**	**0**
Visualcomplexity	2006	0	0	2	0	0	0	**2**	**0**	**0**
Westphal and Blaxton	1998	0	1	1	0	0	0	**2**	**0**	**0**
Wikipedia - Adnan Gulshair el Shukrijumah -	2006	0	1	1	0	0	0	**2**	**0**	**0**
Wikipedia - World Trade Center bombing (1993) -	2006	0	0	0	2	0	0	**2**	**0**	**0**
Wikipedia Riyadh compound bombings	2007	0	0	0	2	0	0	**2**	**0**	**0**
Wikipedia-Bojinka-plot	2006	0	0	1	0	0	0	**1**	**0**	**0**
WorldNetDaily - Wheeler	2003	0	1	0	0	0	0	**1**	**0**	**0**
Xu and Chen	2003	0	0	5	0	1	0	**6**	**0**	**0**
Xu and Chen	2005a	0	0	8	1	0	0	**9**	**0**	**0**
Xu and Chen	2005b	0	0	1	0	0	0	**1**	**0**	**0**
Xu etal	2004	0	1	9	0	0	0	**10**	**0**	**0**
Yang etal	2005	0	0	1	0	0	0	**1**	**0**	**0**
Zhao et al	2006	0	0	2	0	0	0	**2**	**0**	**0**
terrorism research	2005	0	0	1	0	1	0	**2**	**0**	**0**
∑	**-**	**0**	**30**	**171**	**26**	**6**	**0**	**233**	**2**	**0**

Fragments

227 reviewed fragments

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 019 01	19	1, 3-15	Xu and Chen 2003	232	Verschleierung
Nm/Fragment 019 16	19	16-25	Katz et al 2004	308-309	BauernOpfer
Nm/Fragment 020 01	20	1-23	Katz et al 2004	308-309	Verschleierung
Nm/Fragment 021 01	21	1-5	Xu and Chen 2003	233	Verschleierung
Nm/Fragment 023 27	23	27-30	DeRosa 2004	v	BauernOpfer
Nm/Fragment 024 01	24	4-20	DeRosa 2004	v	BauernOpfer
Nm/Fragment 025 22	25	22-29	Koschade_2005	2, 3	Verschleierung
Nm/Fragment 025 30	25	30-32	DeRosa 2004	6	BauernOpfer
Nm/Fragment 026 01	26	1-3	DeRosa 2004	6	BauernOpfer
Nm/Fragment 026 04	26	4-13	Koschade_2005	2, 3	KomplettPlagiat
Nm/Fragment 026 14	26	14-23	Popp and Poindexter 2006	23	Verschleierung
Nm/Fragment 028 05	28	5-8	Xu and Chen 2005a	102	Verschleierung
Nm/Fragment 028 08	28	8-27	Koelle et al 2006	1 (internet version)	KomplettPlagiat
Nm/Fragment 029 03	29	3-8	Tsvetovat et al. 2005	cover	Verschleierung
Nm/Fragment 029 24	29	24-27	DeRosa 2004	6	BauernOpfer
Nm/Fragment 030 01	30	1-26	DeRosa 2004	6-7	BauernOpfer
Nm/Fragment 031 15	31	15-27	Han_Kamber_2006	560, 561, 562	Verschleierung
Nm/Fragment 032 02	32	2-10	Han_Kamber_2006	561, 562	Verschleierung
Nm/Fragment 033 01	33	1-15	Koelle et al 2006	1 (internet version)	KomplettPlagiat
Nm/Fragment 033 15	33	15-30	Ressler 2006	4	KomplettPlagiat
Nm/Fragment 034 01	34	1-9	Ressler 2006	4	Verschleierung
Nm/Fragment 038 01	38	1-3	Ressler 2006	4	Verschleierung
Nm/Fragment 038 04	38	4-23	Koelle et al 2006	2 (internet version)	Verschleierung
Nm/Fragment 038 27	38	27-30	Westphal and Blaxton 1998	201	KomplettPlagiat
Nm/Fragment 039 01	39	1-20	Westphal and Blaxton 1998	201	Verschleierung
Nm/Fragment 040 01	40	1-9	Carley 2006	53	Verschleierung
Nm/Fragment 040 22	40	22-32	Ressler 2006	4, 5	Verschleierung
Nm/Fragment 041 01	41	1-6	Ressler 2006	6	Verschleierung
Nm/Fragment 041 08	41	8-15	Saxena et al. 2004	85	Verschleierung
Nm/Fragment 041 28	41	28-31	Visualcomplexity 2006	1	Verschleierung

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 042 01	42	1-2	Visualcomplexity 2006	1	Verschleierung
Nm/Fragment 042 03	42	3-9	TrackingTheThreat.com 2006	1 (internet version)	Verschleierung
Nm/Fragment 042 12	42	12-18	Saxena et al. 2004	85	Verschleierung
Nm/Fragment 044 18	44	18-22	Ressler 2006	6	KomplettPlagiat
Nm/Fragment 044 23	44	23-30	Hamill_2006	3	Verschleierung
Nm/Fragment 045 01	45	1-16	Carley 2006	51-52	Verschleierung
Nm/Fragment 045 18	45	18-23	Koschade 2005	2 and 3	Verschleierung
Nm/Fragment 046 09	46	9-19	Hamill_2006	9	Verschleierung
Nm/Fragment 047 09	47	9-15	Hamill 2006	11	Verschleierung
Nm/Fragment 047 22	47	22-25	Hamill 2006	11	Verschleierung
Nm/Fragment 048 05	48	5-6	Hamill 2006	11	Verschleierung
Nm/Fragment 049 04	49	3-28	DCSINT_2005	2-10	BauernOpfer
Nm/Fragment 050 01	50	1-21	DCSINT_2005	2-10	BauernOpfer
Nm/Fragment 050 22	50	22-30	Bedi 2005	6	BauernOpfer
Nm/Fragment 051 01	51	1-2, 4-31	Bedi 2005	6-7	BauernOpfer
Nm/Fragment 052 01	52	1-17	Bedi 2005	7	Verschleierung
Nm/Fragment 052 18	52	18-29	Shelley 2002	1	BauernOpfer
Nm/Fragment 053 01	53	1-20	Shelley 2002	1 (internet version)	BauernOpfer
Nm/Fragment 053 21	53	21-30	Shelley 2002	2 (internet version)	KomplettPlagiat
Nm/Fragment 054 01	54	1-12	Shelley 2002	2 (internet version)	KomplettPlagiat
Nm/Fragment 054 13	54	13-23	Shelley 2002	4 (internet version)	Verschleierung
Nm/Fragment 054 23	54	23-32	Shelley 2002	4 (internet version)	Verschleierung
Nm/Fragment 055 01	55	1-7	Shelley 2002	4 (internet version)	Verschleierung
Nm/Fragment 057 11	57	11-29	terrorism_research_2005	1	Verschleierung
Nm/Fragment 058 01	58	1-30	DCSINT_2005	3-1, 3-2	Verschleierung
Nm/Fragment 059 01	59	1-10	DCSINT_2005	3-2	Verschleierung
Nm/Fragment 059 11	59	11-18	DCSINT_2005	3-2	Verschleierung
Nm/Fragment 060 01	60	1-4	DCSINT_2005	3-2	Verschleierung
Nm/Fragment 060 05	60	5-9	DCSINT_2005	3-2	Verschleierung
Nm/Fragment 060 10	60	10-32	DCSINT_2005	3-2, 3-3	Verschleierung

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 061 01	61	1-13	DCSINT_2005	3-3	Verschleierung
Nm/Fragment 061 14	61	14-30	DCSINT_2005	3-4	Verschleierung
Nm/Fragment 062 01	62	1-16	DCSINT_2005	3-4	Verschleierung
Nm/Fragment 062 17	62	17-29	DCSINT_2005	3-4	Verschleierung
Nm/Fragment 063 01	63	1-29	DCSINT_2005	3-4, 3-5	Verschleierung
Nm/Fragment 064 01	64	1	DCSINT_2005	3-5	KomplettPlagiat
Nm/Fragment 064 02	64	2-16	Arquilla_Ronfeldt_2001	69	Verschleierung
Nm/Fragment 065 01	65	1-33	Arquilla_Ronfeldt_2001	69, 70	Verschleierung
Nm/Fragment 066 01	66	1-33	Arquilla_Ronfeldt_2001	70, 71	Verschleierung
Nm/Fragment 067 02	67	2-32	Arquilla_Ronfeldt_2001	71	Verschleierung
Nm/Fragment 068 01	68	1-17	Arquilla_Ronfeldt_2001	71-72	Verschleierung
Nm/Fragment 068 18	68	18-30	DCSINT_2005	2-12	Verschleierung
Nm/Fragment 069 01	69	1-6	DCSINT_2005	2-12	Verschleierung
Nm/Fragment 069 06	69	6-11	Lemieux_2003	5	Verschleierung
Nm/Fragment 069 12	69	12-30	DCSINT_2005	2-12, 2-13	Verschleierung
Nm/Fragment 070 01	70	1-32	DCSINT_2005	2-13	Verschleierung
Nm/Fragment 071 01	71	1-16	DCSINT_2005	2-13, 2-14	Verschleierung
Nm/Fragment 071 17	71	17-32	DCSINT_2005	2-14	Verschleierung
Nm/Fragment 072 01	72	1-26	DCSINT_2005	2-14, 2-15	Verschleierung
Nm/Fragment 072 27	72	27-32	Arquilla_Ronfeldt_2001	72	Verschleierung
Nm/Fragment 073 01	73	1-31	Arquilla_Ronfeldt_2001	72-73	Verschleierung
Nm/Fragment 074 01	74	1-7	Arquilla_Ronfeldt_2001	73	KomplettPlagiat
Nm/Fragment 074 08	74	8-30	Lemieux_2003	6, 12	Verschleierung
Nm/Fragment 075 07	75	7-25	Xu and Chen 2005a	102	Verschleierung
Nm/Fragment 076 01	76	1-17, 20-25, 29-32	Xu and Chen 2005a	102	Verschleierung
Nm/Fragment 077 03	77	3-29	Xu and Chen 2005a	103	BauernOpfer
Nm/Fragment 078 01	78	1-13	Xu and Chen 2005a	103	Verschleierung
Nm/Fragment 079 03	79	3-18	Xu etal 2004	3	Verschleierung
Nm/Fragment 079 19	79	19-29	Clark etal 2005	4	Verschleierung
Nm/Fragment 080 01	80	1-29	Xu etal 2004	3-4	Verschleierung

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 081 01	81	1-32	Xu etal 2004	5	Verschleierung
Nm/Fragment 082 01	82	1-32	Xu etal 2004	5, 6	Verschleierung
Nm/Fragment 083 01	83	1-3	Xu_etal_2004	6	Verschleierung
Nm/Fragment 083 04	83	4-30	CNS_2002	80, 95, 172	Verschleierung
Nm/Fragment 084 01	84	1-10	CNS_2002	172	KomplettPlagiat
Nm/Fragment 084 11	84	11-33	Berry_etal_2004	1, 2	Verschleierung
Nm/Fragment 085 01	85	1-7	Berry_etal_2004	2	Verschleierung
Nm/Fragment 085 08	85	8-27	Clauset_Young_2005	5	Verschleierung
Nm/Fragment 085 28	85	28-32	Xu etal 2004	6	Verschleierung
Nm/Fragment 086 01	86	1-15	Xu etal 2004	6-7	Verschleierung
Nm/Fragment 086 25	86	25-32	Xu etal 2004	7	Verschleierung
Nm/Fragment 087 01	87	1-11	Xu etal 2004	7, 8	Verschleierung
Nm/Fragment 087 12	87	12-32	CNS_2002	18, 105	Verschleierung
Nm/Fragment 088 01	88	1-20	CNS_2002	18, 105	Verschleierung
Nm/Fragment 088 21	88	21-33	Dombroski Carley 2002	1	Verschleierung
Nm/Fragment 089 01	89	1-2	Dombroski Carley 2002	1	Verschleierung
Nm/Fragment 089 03	89	3-25	CNS_2002	14, 18, 20	Verschleierung
Nm/Fragment 090 13	90	13-24	Xu etal 2004	8, 10	KomplettPlagiat
Nm/Fragment 091 11	91	11-20	Ressler 2006	4	Verschleierung
Nm/Fragment 091 21	91	21-28	Ressler 2006	4, 5	Verschleierung
Nm/Fragment 093 04	93	4-16	Xu_and_Chen_2003	232	Verschleierung
Nm/Fragment 093 17	93	17-25	Katz et al 2004	308	Verschleierung
Nm/Fragment 094 01	94	1-25	Katz et al 2004	308-309	Verschleierung
Nm/Fragment 094 28	94	28-32	Xu and Chen 2003	232	Verschleierung
Nm/Fragment 095 01	95	1-8	Xu and Chen 2003	233	Verschleierung
Nm/Fragment 095 12	95	12-15	Borgatti_2002	1	KomplettPlagiat
Nm/Fragment 096 02	96	2-20	Borgatti_2002	2	Verschleierung
Nm/Fragment 097 01	97	1-8	Borgatti_2002	2	Verschleierung
Nm/Fragment 097 09	97	9-19	Brandes_Erlebach_2005	7, 8	Verschleierung
Nm/Fragment 098 09	98	9-22	Borgatti_2002	3	KomplettPlagiat

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 099 01	99	1-25	Borgatti_2002	3-4	Verschleierung
Nm/Fragment 099 26	99	26-32	Brandes_Erlebach_2005	8	KomplettPlagiat
Nm/Fragment 100 01	100	1-16	Brandes_Erlebach_2005	8, 9	Verschleierung
Nm/Fragment 100 24	100	24-30	Stephenson and Zelen 1989	2-3	Verschleierung
Nm/Fragment 101 01	101	1-8	Scott_1987	23	Verschleierung
Nm/Fragment 101 20	101	20-26	Koschuetzki_etal_2005	20	KomplettPlagiat
Nm/Fragment 102 02	102	2-28	Scott_1987	83-85	Verschleierung
Nm/Fragment 103 15	103	15-27	Koschuetzki_etal_2005	22-23	Verschleierung
Nm/Fragment 104 02	103	2-8	Stephenson and Zelen 1989	3	Verschleierung
Nm/Fragment 104 12	104	12-24	Koschuetzki_etal_2005	29-30	Verschleierung
Nm/Fragment 106 14	106	14-17	Balasundaram et al 2006	2	Verschleierung
Nm/Fragment 107 01	107	1-4	Balasundaram et al 2006	2	KomplettPlagiat
Nm/Fragment 107 07	107	7-23	Penzar_etal_2005	33-34	Verschleierung
Nm/Fragment 108 02	108	2-19	Penzar_etal_2005	34	Verschleierung
Nm/Fragment 109 01	109	1-13	Penzar_etal_2005	34, 35	Verschleierung
Nm/Fragment 111 17	111	17-27	Holmgren 2006	956	KomplettPlagiat
Nm/Fragment 112 01	112	1-27	Holmgren 2006	956-957	KomplettPlagiat
Nm/Fragment 113 01	113	1-22	Holmgren 2006	957	KomplettPlagiat
Nm/Fragment 113 23	113	23-27	Chen 2006	98	Verschleierung
Nm/Fragment 114 01	114	1-12	Chen 2006	98-99	Verschleierung
Nm/Fragment 114 13	114	13-19	Chen 2006	98	Verschleierung
Nm/Fragment 114 20	114	20-33	Krebs 2004	1 (internet version)	BauernOpfer
Nm/Fragment 115 01	115	1-3	Krebs 2004	1 (internet version)	BauernOpfer
Nm/Fragment 115 04	115	4-10	Chen 2006	99-100	Verschleierung
Nm/Fragment 115 12	115	12-23	Qin et al 2005	299	BauernOpfer
Nm/Fragment 117 01	117	1-2, 3-8	Chen 2006	98	Verschleierung
Nm/Fragment 118 08	118	8, 12-25	Latora and Marchiori 2004	70	BauernOpfer
Nm/Fragment 125 01	125	1-29	Wikipedia_Riyadh_compound_bombings_2007	1 (internet version)	BauernOpfer
Nm/Fragment 126 01	126	1-10	Wikipedia_Riyadh_compound_bombings_2007	1 (internet version)	BauernOpfer
Nm/Fragment 138 12	138	12-20	Freeman 1980	587	Verschleierung

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 139 11	139	11-14	Freeman 1980	588	Verschleierung
Nm/Fragment 140 01	140	1-6	Freeman 1980	588	Verschleierung
Nm/Fragment 143 02	143	2-5	Stephenson and Zelen 1989	26-27	Verschleierung
Nm/Fragment 144 13	144	13-15	Stephenson and Zelen 1989	27	KomplettPlagiat
Nm/Fragment 144 16	144	16-21	Stephenson and Zelen 1989	3	KomplettPlagiat
Nm/Fragment 146 03	146	3-15	Penzar_etal_2005	28	Verschleierung
Nm/Fragment 146 20	146	20-25	Combating Terrorism Center 2006	8	Verschleierung
Nm/Fragment 147 01	147	1-13	Combating Terrorism Center 2006	8	BauernOpfer
Nm/Fragment 147 18	147	18-29	Yang_etal_2005	2	Verschleierung
Nm/Fragment 162 03	162	3-8	Krebs 2002	46	Verschleierung
Nm/Fragment 165 01	165	1, 3-6	Latora and Marchiori 2004	73	Verschleierung
Nm/Fragment 166 11	166	11-18	WorldNetDaily - Wheeler 2003	1 (internet version)	KomplettPlagiat
Nm/Fragment 168 03	168	3-13	Wikipedia - Adnan Gulshair el Shukrijumah - 2006	1 (internet version)	KomplettPlagiat
Nm/Fragment 169 01	169	1-10	Wikipedia - Adnan Gulshair el Shukrijumah - 2006	1 (internet version)	Verschleierung
Nm/Fragment 170 02	170	2-7	Wikipedia - World Trade Center bombing (1993) - 2006	1 (internet version)	BauernOpfer
Nm/Fragment 171 01	171	1-4	Wikipedia - World Trade Center bombing (1993) - 2006	1 (internet version)	BauernOpfer
Nm/Fragment 174 02	174	2-16	Wikipedia-Bojinka-plot_2006	1	Verschleierung
Nm/Fragment 178 05	178	5-15	Perer_Shneiderman_2006	693	Verschleierung
Nm/Fragment 180 02	180	2-16	Perer_Shneiderman_2006	693	Verschleierung
Nm/Fragment 181 01	181	1-33	Perer_Shneiderman_2006	693	Verschleierung
Nm/Fragment 182 01	182	1-33	Perer_Shneiderman_2006	694	Verschleierung
Nm/Fragment 183 01	183	1-14	Perer_Shneiderman_2006	694	Verschleierung
Nm/Fragment 183 17	183	17-24	Heer et al 2005	1 (internet version)	Verschleierung
Nm/Fragment 183 25	183	25-28	Heer et al 2005	3 (internet version)	BauernOpfer
Nm/Fragment 184 09	184	9-11, 12-15	Heer et al 2005	3 (internet version)	Verschleierung
Nm/Fragment 185 01	185	1-27	Heer et al 2005	3-4 (internet version)	Verschleierung
Nm/Fragment 186 03	186	3-32	Heer et al 2005	4	Verschleierung
Nm/Fragment 187 01	187	1-31	Heer et al 2005	4-5 (internet version)	Verschleierung
Nm/Fragment 188 01	188	1-30	Heer et al 2005	5 (internet version)	Verschleierung
Nm/Fragment 189 01	189	1-29	Heer et al 2005	5 (internet version)	Verschleierung

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 190 03	190	3-16	Heer et al 2005	5 (internet version)	Verschleierung
Nm/Fragment 190 17	190	17-31	Heer et al 2005	9 (internet version)	Verschleierung
Nm/Fragment 191 01	191	1-6	Heer et al 2005	10 (internet version)	Verschleierung
Nm/Fragment 191 10	191	10-19	Xu and Chen 2005a	104-105	Verschleierung
Nm/Fragment 191 20	191	20-25	Xu and Chen 2005a	106	Verschleierung
Nm/Fragment 192 01	192	1-12	Smith and King 2002	5 (internet version)	Verschleierung
Nm/Fragment 193 01	193	1-12	Smith and King 2002	6 (internet version)	Verschleierung
Nm/Fragment 194 01	194	1-7	Smith and King 2002	6 (internet version)	Verschleierung
Nm/Fragment 195 02	195	2-12	Smith and King 2002	7 (internet version)	Verschleierung
Nm/Fragment 198 03	198	3-18	Xu and Chen 2005b	201	Verschleierung
Nm/Fragment 199 10	199	10-15	Perer_Shneiderman_2006	693	Verschleierung
Nm/Fragment 199 27	199	27-28	Xu and Chen 2005a	106	Verschleierung
Nm/Fragment 200 01	200	1-4	Xu and Chen 2005a	106	Verschleierung
Nm/Fragment 202 12	202	12-21	Tsvetovat et al. 2005	2	Verschleierung
Nm/Fragment 205 21	205	21-23	Zhao et al 2006	2	Verschleierung
Nm/Fragment 206 01	206	1-21	Zhao et al 2006	2	Verschleierung
Nm/Fragment 206 26	206	26-28	Jensen et al 2003	381	KomplettPlagiat
Nm/Fragment 207 01	207	1-6	Jensen et al 2003	381	KomplettPlagiat
Nm/Fragment 207 12	207	12-18, 20, 21-22	Frost 1982	358	KomplettPlagiat
Nm/Fragment 208 01	208	1-10	Frost 1982	359	BauernOpfer
Nm/Fragment 208 11	208	11-15, 17-18, 24-28	Frost 1982	360-361	Verschleierung
Nm/Fragment 214 02	214	2-7	TrackingTheThreat.com 2006a	1 (internet version)	Verschleierung
Nm/Fragment 214 07	214	7-14	TrackingTheThreat.com 2006	1 (internet version)	KomplettPlagiat
Nm/Fragment 214 15	214	15-24	TrackingTheThreat.com 2006	1 (internet version)	Verschleierung
Nm/Fragment 215 01	215	1-4	Dugan_etal_2006	409	Verschleierung
Nm/Fragment 215 11	215	11-31	Malin_etal_2005	119, 120	Verschleierung
Nm/Fragment 216 05	216	5-30	Dugan_etal_2006	410-411	Verschleierung
Nm/Fragment 219 04	219	4-8, 10-23, 24-26	Balasundaram et al 2006	1, 2	Verschleierung
Nm/Fragment 219 27	219	27-28	Stokman_2004	1	Verschleierung
Nm/Fragment 220 01	220	1-14	Stokman_2004	1	Verschleierung

Fragment	SeiteArbeit	ZeileArbeit	Quelle	SeiteQuelle	Typus
Nm/Fragment 220 14	220	14-29	Aviv et al 2003	4	Verschleierung
Nm/Fragment 221 23	221	23-29	Balasundaram et al 2006	2	Verschleierung
Nm/Fragment 222 01	222	1-25	Balasundaram et al 2006	2	Verschleierung
Nm/Fragment 231 10	231	10-14	Aviv et al 2003	10	KomplettPlagiat
Nm/Fragment 239 10	239	10-20	Hamill_2006	278	Verschleierung
Nm/Fragment 240 24	240	24-26	Hamill_2006	278	Verschleierung
Nm/Fragment 241 01	241	1-3	Hamill 2006	278	Verschleierung
Nm/Fragment 242 09	242	9-14	Stephenson and Zelen 1989	3	KomplettPlagiat
Nm/Fragment 243 23	243	23-26	Saxena et al. 2004	94	Verschleierung
Nm/Fragment 244 21	244	21-32	Ressler 2006	7	BauernOpfer
Nm/Fragment 245 01	245	1-5	Ressler 2006	7	Verschleierung
Nm/Fragment 246 08	246	8-28	Lemieux_2003	12-13	Verschleierung
Nm/Fragment 247 01	247	1-21	Lemieux_2003	13	Verschleierung
Nm/Fragment 247 22	247	22-29	Ressler 2006	7-8	Verschleierung
Nm/Fragment 248 01	248	1-9	Ressler 2006	8	Verschleierung
Nm/Fragment 248 24	248	24-28	Hamill_2006	285	Verschleierung
Nm/Fragment 249 01	249	1-8	Hamill_2006	285	Verschleierung

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. However, charts and tables, including their captions, are usually not counted.

227 reviewed fragments

[1.] Nm/Fragment 019 01

Verschleierung

Untersuchte Arbeit: Seite: 19, Zeilen: 1, 3-15	Quelle: Xu and Chen 2003 Seite(n): 232, Zeilen: 21-23, 24-29, 30-32
I. INTRODUCTION [FN 1] **1.1. OVERVIEW** Terrorists seldom operate in vacuum but interact with one another to carry out terrorist activities. To perform terrorist activities requires collaboration among terrorists. Relationship between individual terrorists for the basis of terrorism and are essential for the smooth operation of a terrorist organization, which can be viewed as network consisting of nodes [FN 2] (for example terrorists, terrorist camps, supporting countries, etc.) and links [FN 3] / ties (relationships). In terrorist networks, there may present some groups/ or cells, 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. Some others may serve as gatekeepers to ensure smooth flow of information or illicit goods. [FN 1] Parts of this chapter are already published in Memon N., Hicks David L., and Larsen Henrik Legind. (2007d) Memon N. Lasen H.L. (2006a) (2006b) (2006c); [FN 2] In this dissertation the words: nodes, actors, players, and vertices are used interchangeably [FN 3] In this dissertation the words: links, ties, relationships, and edges are used interchangeably	**1 Introduction** Criminals seldom operate in a vacuum but interact with one another to carry out various illegal activities. In particular, organized crimes [...] 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 [...]. 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

Take somebody else's introduction, shorten it slightly, cross out "criminals" and "offenders" and put "terrorists" instead. That way Nm's introduction was made. (There is no reference to Xu and Chen (2003))

The whole page will be repeated more or less on page 93 of the thesis: Nm/Fragment_093_04

[2.] Nm/Fragment 019 16

BauernOpfer

Untersuchte Arbeit: Seite: 19, Zeilen: 16-25	Quelle: Katz et al 2004 Seite(n): 308-309, Zeilen: p.308,23-33 - p.309,1-2
In social network literature, researchers have examined a broad range of types of ties (Katz, N. et al. 2004). 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 foot-[soldier / newly recruited person in terrorist cell and reports to the other, who is the cell leader) and an affective tie (they are friends) and proximity tie (they are residing in the same apartment and their flats are two doors away on the same floor).]	[p. 308] 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, 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) [p. 309] and an affective tie (they are friends) and a proximity tie (their offices are two doors away).

Farbig

Anmerkungen

The exact same section will be used again on pages 93 and 94 of this thesis [4], [5]. Here like there, there is only a passing reference made to the source of this text. Here like there, nothing is marked as a citation.

[3.] Nm/Fragment 020 01

Verschleierung

Untersuchte Arbeit: **Seite: 20, Zeilen: 1-23**	**Quelle: Katz et al 2004** **Seite(n): 308-309, Zeilen: p.308,31-33 - p.309,1-11.13-20**

Farbig

[For example, two terrorists might have a formal tie (one is foot-]soldier / newly recruited person in terrorist cell and reports to the other, who is the cell leader) and an affective tie (they are friends) and proximity tie (they are residing in the same apartment and their flats are two doors away on the same floor).

Network researchers have made a difference between strong ties (such as wife and husband) and weak ties such as colleagues met at a conference (Granovetter, 1973, 1982). This distinction includes affect, mutual obligations, reciprocity, and intensity. Strong ties become valuable when an individual pursues socio-emotional support and should be trustworthy. On the other hand, weak ties become valuable when individuals pursue varied or unique information from external outside their routine contacts.

As per study of the literature, this study found that the ties may be non-directional (*Atta* attends meeting with *Nawaf Alhazmi*) or differ in direction (*Bin Laden* gives advice to *Atta* vs. *Atta* gets advice from *Bin Laden*). They may differ in content (*Atta* talks with *Khalid* about the trust of his friends (to be used as human bombs for 9/11) and *Khalid* about his meeting with *Bin Laden*), frequency (daily, weekly, monthly, etc.), and medium (frontal conversation, written memos, email, fax, instant messages, live chat, Skype or Facebook messages, etc.). Finally ties may differ in sign, ranging from positive (*Iraqis* like *Zarqawi*) to negative (*Jordanians* dislike *Zarqawi*).

[p. 308]

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)

[p.309]

and an affective tie (they are friends) and a proximity tie (their offices are two doors away).

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. [...]

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).

Anmerkungen

To be found again here [6].

[4.] Nm/Fragment 021 01

Verschleierung

Untersuchte Arbeit: Seite: 21, Zeilen: 1-5	Quelle: Xu and Chen 2003 Seite(n): 233, Zeilen: 1-4
[For example, arrest of central members in a network may affect the operation of a network and put a] terrorist organization out of action (Baker, W. E., Faulkner R. R., 1993; McAndrew, D., 1999; Sparrow, M. K., 1991). Subgroups and interaction patterns between groups are helpful in detecting overall structure of a network (Evan, W. M., 1972; Ronfeldt, D., Arquilla, J., 2001).	[For exam]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].

Farbig

[EN 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.

[EN 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.

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

[EN 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.

[EN 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).

Anmerkungen

Content, references and a number of formulations are identical though the source refers to criminals, Nm to terrorists. This section also appears at Nm/Fragment 095 01.

[5.] Nm/Fragment 023 27

BauernOpfer

Untersuchte Arbeit: Seite: 23, Zeilen: 27-30	Quelle: DeRosa 2004 Seite(n): v, Zeilen: 2-5
Defeating terrorist networks requires a more nimble intelligence apparatus that operates more actively and makes use of advanced information technology. Data mining for counterterrorism (In the study we call it as investigative data mining [FN 4]) is a powerful tool for [intelligence and law enforcement officials fighting terrorism (DeRosa Mary, 2004).]	Defeating terrorism requires a more nimble intelligence apparatus that operates more actively within the United States and makes use of advanced information technology. Data-mining and automated data-analysis techniques are powerful tools for intelligence and law enforcement officials fighting terrorism.

Farbig

[FN 4] The term is firstly used by Jesus Mena in his book Investigative Data Mining and [Criminal Detection, Butterworth (2003).]

Anmerkungen

Although the source is given nothing is marked as a citation.

[6.] Nm/Fragment 024 01

BauernOpfer

Untersuchte Arbeit: **Seite: 24, Zeilen: 4-20**	**Quelle: DeRosa 2004** **Seite(n): v, Zeilen: 19-25, 32-38**
Data mining actually has relatively narrow meaning: the approach that uses algorithms to determine analytical patterns in datasets. Subject-based automated data analysis applies models to data to predict behaviour, assess risk, determine associations, or do other type of analysis (DeRosa Mary, 2004). The models used for automated data analysis can be used on patterns discovered by data mining techniques.	"Data mining" actually has a relatively narrow meaning: it is a process that uses algorithms to discover predictive patterns in data sets. "Automated data analysis" applies models to data to predict behavior, assess risk, determine associations, or do other types of analysis. The models used for automated data analysis can be based on patterns (from data mining or discovered by other methods) or subject based, which start with a specific known subject. [...]
Although these techniques are powerful, it is a mistake to view investigative data mining techniques as complete solution to security problems. The strength of investigative data mining (IDM) is to assist analysts and investigators. IDM can automate some tasks that analysts would otherwise have to accomplish manually. It can help to place in order attention and focus an inquiry, and can even do some early analysis and sorting of masses of data. Nevertheless, in the multifaceted 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

Every now and then a reference to the source is thrown in. Nevertheless nothing of the cited text is marked as such.

[7.] Nm/Fragment 025 22

Verschleierung

Untersuchte Arbeit: **Seite: 25, Zeilen: 22-29**	**Quelle: Koschade_2005** **Seite(n): 2, 3, Zeilen: p2:6-8; p3:31-35**
IDM offers ability to map a covert cell, and to measure the specific structural and interactive criteria of such a cell. This framework aims to connect dots between individuals and to map and measure complex, covert, human groups and organisations (Memon N., and Larsen H. L., 2006c). 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 (Memon N., and Larsen H. L., 2006c).	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". [EN 8] The method focuses on uncovering the patterning of people's interaction, [EN 9] and correctly interpreting these networks assists "in predicting behaviour and decision-making within the network". [EN 10] --- [EN 8] Krebs, V. (2002) "Mapping Networks of Terrorist Cells", Connections, Vol. 24, 3, pp. 43-52. [EN 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. [EN 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.

Farbig

Anmerkungen

The source is not mentioned anywhere in the thesis.

Not only did Nm copy an entire paragraph from the source, he also references for it the paper "Memon N., and Larsen H. L., 2006c", written by himself and the thesis supervisor. Finally he also removes the references for correct quotations in the source.

[8.] Nm/Fragment 025 30

BauernOpfer

Untersuchte Arbeit: Seite: 25, Zeilen: 30-32	Quelle: DeRosa 2004 Seite(n): 6, Zeilen: 25-29
This technique is also known as subject based link analysis. This technique uses aggregated public records or other large collection of data to find the links between a subject — a suspect, an address, [or a piece of relevant information — and other people, places, or things.]	A relatively simple and useful data-analysis tool for counterterrorism is subject-based “link analysis.” This technique uses aggregated public records or other large collections of data to find links between a subject — a suspect, an address, or other piece of relevant information — and other people, places, or things.

Farbig

Anmerkungen

At the end of the paragraph (on the next page) the source is given. Unfortunately nothing in this paragraph has been marked as a citation.

[9.] Nm/Fragment 026 01

BauernOpfer

Untersuchte Arbeit: Seite: 26, Zeilen: 1-3	Quelle: DeRosa 2004 Seite(n): 6, Zeilen: 26-29
[This technique uses aggregated public records or other large collection of data to find the links between a subject—a suspect, an address,] or a piece of relevant information—and other people, places, or things. This can provide additional clues for analysts and investigators to follow (DeRosa Mary, 2004).	This technique uses aggregated public records or other large collections of data to find links between a subject—a suspect, an address, or other piece of relevant information—and other people, places, or things. This can provide additional clues for analysts and investigators to follow.

Farbig

Anmerkungen

continuation of previous fragment

[10.] Nm/Fragment 026 04

KomplettPlagiat

Untersuchte Arbeit: Seite: 26, Zeilen: 4-13	Quelle: Koschade_2005 Seite(n): 2, 3, Zeilen: p2: 8-13: p3:38-40
IDM also gives the analyst 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. In short, IDM provides a useful way of structuring knowledge and framing further research. Ideally it can also enhance an analyst’s predictive capability (Memon N., and Larsen H. L., 2006c).	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”.[EN 12] --- [EN 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.

Farbig

Anmerkungen

The source is not mentioned anywhere in the thesis.

Not only did Nm copy an entire paragraph from the source, he also references for it the paper "Memon N., and Larsen H. L., 2006c", written by himself and the thesis supervisor. Finally he also removes the reference to Aftergood (2004) who Koschade correctly quotes for the last sentence.

[11.] Nm/Fragment 026 14

Verschleierung

Untersuchte Arbeit: Seite: 26, Zeilen: 14-23	Quelle: Popp and Poindexter 2006 Seite(n): 23, Zeilen: left column 5-16
Traditional data mining normally refers to using techniques rooted in statistics, rule-based logic, or artificial intelligence, machine learning, fuzzy logic, statistics to examine through large amounts of data to find previously unknown but statistically significant patterns. However, the application of IDM in the counterterrorism domain is more challenging, because unlike traditional data mining applications, we must find extremely wide variety of activities and hidden relationships among individuals (Seifert 2006). Table 1.1 gives a series of reasons why traditional data mining is not 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

no source given

[12.] Nm/Fragment 028 05

Verschleierung

Untersuchte Arbeit: Seite: 28, Zeilen: 5-8	Quelle: Xu and Chen 2005a Seite(n): 102, Zeilen: left column 42-46
Although SNA is not conventionally considered as data mining technique, it is especially suitable for mining a large volume of association data to discover hidden structural patterns in terrorist networks.	Although SNA is not traditionally considered as a data mining technique, it is especially suitable for mining large volumes of association data to discover hidden structural patterns in criminal networks [9, 10].

Farbig

Anmerkungen

Right before he starts to massively present material form Koelle et al. (2006), for which he gives no reference, he puts in a small section, adapted in the usual way, from Xu and Chen (2005a), which he also does not mark as a citation and for which he also does not give a reference.

Pure patchwork.

[13.] Nm/Fragment 028 08

KomplettPlagiat

Untersuchte Arbeit: Seite: 28, Zeilen: 8-27	Quelle: Koelle et al 2006 Seite(n): 1 (internet version), Zeilen: left column 25-46
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 and 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 and Faust, 1994).	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).
SNA is used in a variety of domains. For example, business consultants use SNA to identify the effective relationships between workers that enable work to get done; these relationships often differ from connections seen in an organizational chart (Ehrlich and Carboni, 2005). Law enforcement personnel have used social networks to analyze terrorist networks (Krebs, 2002; Stewart, 2001) and criminal networks (Sparrow, M. K., 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).	SNA is used in a variety of domains. For example, business consultants use SNA to identify the effective relationships between workers that enable work to get done; these relationships often differ from connections seen in an organizational chart (Ehrlich & Carboni, 2005). 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).

Farbig

Anmerkungen

Identical, with the source not even being mentioned in Nm's thesis.

[14.] Nm/Fragment 029 03

Verschleierung

Untersuchte Arbeit: **Seite: 29, Zeilen: 3-8**	**Quelle: Tsvetovat et al. 2005** **Seite(n): cover, Zeilen: 10ff**	Farbig
There is a pressing need to automatically collect data of terrorist networks, analyze such networks to find hidden relations and groups, prune datasets to locate regions of interest, detect key players, characterize the structure, trace points of vulnerability, and find efficiency (how fast communication is being made) of the network.	There is a pressing need to automatically collect data on social systems as rich network data, analyze such systems to find hidden relations and groups, prune the datasets to locate regions of interest, locate key actors, characterize the structure, locate points of vulnerability, and simulate change in a system as it evolves naturally or in response to strategic interventions over time or under certain impacts, including modifcation of data.	

Anmerkungen

Only the last half-sentence is substantially different to the source, which is not mentioned anywhere in the thesis.

[15.] Nm/Fragment 029 24

BauernOpfer

Untersuchte Arbeit: **Seite: 29, Zeilen: 24-27**	**Quelle: DeRosa 2004** **Seite(n): 6, Zeilen: 33-38**	Farbig
Taking an example of 9/11 attack, it is possible to show, that simple IDM techniques discussed above can be used to assist terrorist investigation. IDM techniques using government watch list information, airline reservation records, and aggregated public [record data, could have identified all 19 hijackers of 9/11 terrorists attacks before the attack. (DeRosa Mary, 2004):]	A hindsight analysis of the September 11 attacks provides an example of how simple, subject-based link analysis could be used effectively to assist investigations or analysis of terrorist plans. By using government watch list information, airline reservation records, and aggregated public record data, link analysis could have identified all 19 September 11 terrorists — for follow-up investigation — before September 11. [FN 16] --- [FN 16] Of course, this kind of analysis will always appear neater and easier with hindsight, but it is a useful demonstration nonetheless.	

Anmerkungen

Only a cursory reference to the source is made, and it is not clear if it refers to what has come before or to what will come; nothing is marked as a citation.

[16.] Nm/Fragment 030 01

BauernOpfer

Untersuchte Arbeit: **Seite: 30, Zeilen: 1-26**	**Quelle: DeRosa 2004** **Seite(n): 6-7, Zeilen: p.6,26-27 - p.7,1-25**

Farbig

[IDM techniques using government watch list information, airline reservation records, and aggregated public] record data, could have identified all 19 hijackers of 9/11 terrorists attacks before the attack. (DeRosa Mary, 2004):

The details about these links can be summarized as follows:

• Watch List Information (Direct Links)

o *Khalid Almindhar and Nawaf Alhazmi*, both were involved in 9/11 hijacking and were on U.S. government terrorist watch list.

o *Ahmed Alghamdi*, who hijacked United Airlines (UA) Flight 175, and crashed it into the World Trade Center South Tower, was on an Immigration and Naturalization Service (INS) watch list for illegal or expired visas.

It is noteworthy to specify all three of the above given terrorists used their real names to reserve the flights.

• Link Analysis (One Degree of Separation)

o *Muhammad Atta and Mavan Al shehhi*, both hijackers used same contact address for their flight reservations that Khalid Almihdhar used for his flight reservation.

o *Salem Alhazmi*, used the same contact address on his reservation as Nawaf Alhazmi.

o *Majed Moqed* used the same frequent flyer number that Khalid Al mindhar used in his reservation.

o *Hamza Alghamdi*, used the same contact address on his reservation as Ahmed Alghamdi used on his reservation.

o *Hani Hanjour*, lived with both Nawaf Alhazmi and Khalid Almihdhar, a fact that searches of public records could have revealed.

[p. 6]

By using government watch list information, airline reservation records, and aggregated public record data, link analysis could have identified all 19 September 11 terrorists—for follow-up investigation—before September 11. [FN 16] The links can be summarized as follows:

[p. 7]

Direct Links — Watch List Information

Khalid Almihdhar and **Nawaf Alhazmi**, both hijackers of American Airlines (AA) Flight 77, which crashed into the Pentagon, appeared on a U.S. government terrorist watch list. Both used their real names to reserve their flights.

Ahmed Alghamdi, who hijacked United Airlines (UA) Flight 175, which crashed into the World Trade Center South Tower, was on an Immigration and Naturalization Service (INS) watch list for illegal or expired visas. He used his real name to reserve his flight.

Link Analysis — One Degree of Separation

Two other hijackers used the same contact address for their flight reservations that Khalid Almihdhar listed on his reservation. These were **Mohamed Atta**, who hijacked AA Flight 11, which crashed into the World Trade Center North Tower, and **Marwan Al Shehhi**, who hijacked UA Flight 175.

Salem Alhazmi, who hijacked AA Flight 77, used the same contact address on his reservation as Nawaf Alhazmi.

The frequent flyer number that Khalid Almihdhar used to make his reservation was also used by hijacker **Majed Moqed** to make his reservation on AA Flight 77.

Hamza Alghamdi, who hijacked UA Flight 175, used the same contact address on his reservation as Ahmed Alghamdi used on his.

Hani Hanjour, who hijacked AA Flight 77, lived with both Nawaf Alhazmi and Khalid Almihdhar, a fact that searches of public records could have revealed.

Anmerkungen

continued from previous page; most formulations are taken from the original, nothing is marked as a citation.

[17.] Nm/Fragment 031 15

Verschleierung

Untersuchte Arbeit: Seite: 31, Zeilen: 15-27	Quelle: Han_Kamber_2006 Seite(n): 560, 561, 562, Zeilen: 560: 37-38; 561: 1-8; 562: 27-29
"How can we mine terrorist networks?" Traditional methods of machine learning and data mining, taking, as input, a random sample of homogeneous objects from a single relation, may not be appropriate here. The data comprising terrorist networks tend to be heterogeneous, multi-relational, and semi-structured. IDM embodies descriptive and predictive modeling. By considering links (the relationship between the objects), the more information is made available to the mining process. This brings about several new tasks. Here we list these tasks. (1) **Group detection.** Group detection is a clustering task. It predicts when sets of objects belong to the same group or cluster, based on their attributes as well as their link [structure.]	"How can we mine social networks?" Traditional methods of machine learning and data mining, taking, as input, a random sample of homogenous objects from a single [page 561] relation, may not be appropriate here. The data comprising social networks tend to be heterogeneous, multirelational, and semi-structured. [...] It embodies descriptive and predictive modeling. By considering links (the relationships between objects), more information is made available to the mining process. This brings about several new tasks. Here, we list these tasks with examples from various domains: [page 562] [...] 7. **Group detection.** Group detection is a clustering task. It predicts when a set of objects belong to the same group or cluster, based on their attributes as well as their link structure.

Farbig

Anmerkungen

Taken from a textbook on data-mining without reference.

[18.] Nm/Fragment 032 02

Verschleierung

Untersuchte Arbeit: Seite: 32, Zeilen: 2-10	Quelle: Han_Kamber_2006 Seite(n): 561, 562, Zeilen: -
(2) **Sub-graph detection**. Subgraph identification finds characteristic subgraphs within networks. This is a form of graph search and also known as graph filtering technique. (3) **Object classification**. In traditional classification methods, objects are classified on the attributes that describe them. Link-based classification predicts the category of an object-based not only on attributes, but also on links, and on the attributes of the linked objects.	[page 562] 8. **Subgraph detection**. Subgraph identification finds characteristic subgraphs within networks. This is a form of graph search and was described in Section 9.1. [page 561] 1. **Link-based object classification**. In traditional classification methods, objects are classified based on the attributes that describe them. Link-based classification predicts the category of an object based not only on its attributes, but also on its links, and on the attributes of linked objects.

Farbig

Anmerkungen

Taken from a textbook on data-mining without reference

[19.] Nm/Fragment 033 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 33, Zeilen: 1-15	Quelle: Koelle et al 2006 Seite(n): 1 (internet version), Zeilen: right column 26-43
1.5. LIMITATIONS	**2. LIMITATIONS OF SOCIAL NETWORK ANALYSIS**
While traditional SNA has been used to successfully derive insights into a social network, it can be restrictive for a number of reasons. SNA assumes a well-formed social network, but real-world methods of data collection may not ensure that the resulting social network is complete and contains needed data. SNA focuses primarily on the existence of a relationship between nodes in the network, but not on attributes of that relationship or the nodes in the relationship. Furthermore, SNA does not explicitly consider the uncertainty of attributes on nodes or relationships. Finally, graph-theoretic algorithms used in SNA tend to focus on homogenous set of entities and relationships, making it difficult to analyze networks that involve a heterogeneous set of nodes connected by a variety of link types.	While traditional SNA has been used to successfully derive insights into a social network, it can be restrictive for a number of reasons. SNA assumes a well-formed social network, but real-world methods of data collection may not ensure that the resulting social network is complete and contains needed data. SNA focuses primarily on the existence of a relationship between nodes in the network, but not on attributes of that relationship or the nodes in the relationship. Furthermore, SNA does not explicitly consider the uncertainty of attributes on nodes or relationships. Finally, graph-theoretic algorithms used in SNA tend to focus on a homogenous set of entities and relationships, making it difficult to analyze networks that involve a heterogeneous set of nodes connected by a variety of link types.
1.5.1 Issues in Data Collection [FN 7]	**2.1 ISSUES IN DATA COLLECTION**
[FN 7] The text in this subsection is partially published in Memon Nasrullah and Larsen Henrik Legind. (2007e)	

Farbig

Anmerkungen

Identical, with the source not being mentioned anywhere in Nm's thesis.

[20.] Nm/Fragment 033 15

KomplettPlagiat

Untersuchte Arbeit: Seite: 33, Zeilen: 15-30	Quelle: Ressler 2006 Seite(n): 4, Zeilen: 7-19
1.5.1 Issues in Data Collection[FN 7]	**Data Collectors**
Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling. Valdis Krebs was one of the first to collect data using public sources with his 2001 article in Connections. In this work, Krebs creates a pictorial representation of the al Qaeda network (as shown in Figure 1.4) responsible for 9/11 that shows the many connections between the hijackers of the four airplanes. Similarly, After the Madrid bombing in 2004, Spanish sociologist Jose A. Rodriguez conducted an analysis to map the March 11th terrorist network.	Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling. Valdis Krebs was one of the first to collect data using public sources with his 2001 article in Connections. In this work, Krebs creates a pictorial representation of the al Qaeda network responsible for 9/11 that shows the many ties between the hijackers of the four airplanes. After the Madrid bombing in 2004, Spanish sociologist Jose A. Rodriguez completed an analysis similar to Krebs' by using public sources to map the March 11th terrorist network.
[FN 7] The text in this subsection is partially published in Memon Nasrullah and Larsen Henrik Legind. (2007e)	

Farbig

Anmerkungen

The conference, the proceedings of which "this subsection is partially published" in, was held on 4-6 July 2007. Thus the unnamed source predates (again) the text by Nm. It should also be noticed that the coauthors of the conference paper by Nm are his thesis advisor and the chair of his thesis committee.

Note: in the bibliography there are two entries (2007e): "Memon Nasrullah and Larsen Henrik Legind. (2007e)" as well as "Memon Nasrullah, Hicks David L., and Larsen Henrik Legind (2007e)". Only the latter has common text fragments with the chapter 1.5.1 of the dissertation and therefore it was assumed that in FN 7 this publication was meant.

[21.] Nm/Fragment 034 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 34, Zeilen: 1-9	Quelle: Ressler 2006 Seite(n): 4, Zeilen: 21-25, 32-35
Understanding Terror Networks by Marc Sageman was another brilliant attempt in this regard. He using public sources, collected biographies of 172 Islamic terrorist operatives affiliated with the global Salafi jihad (the violent revivalist Islamic movement led by al Qaeda). He also used social network analysis specifically on Al Qaeda operatives since 1998. However collecting terrorists' information from open sources has a few key drawbacks. With open sources, if the author does not have information on terrorists, he or she assumes they do not exist.	Another bright spot is the 2004 publication of *Understanding Terror Networks* by Marc Sageman. Using public sources, Sageman collects biographies of 172 Islamic terrorist operatives affiliated with the global Salafi jihad (the violent revivalist Islamic movement led by al Qaeda). He uses social network analysis specifically on Al Qaeda operatives since 1998. [...] Despite their many strengths, Krebs' and Sageman's works have a few key drawbacks. By dealing with open sources, these authors are limited in acquiring data. With open sources, if the author does not have information on terrorists, he or she assumes they do not exist.

Anmerkungen

Continued from previous page.

[22.] Nm/Fragment 038 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 38, Zeilen: 1-3	Quelle: Ressler 2006 Seite(n): 4, Zeilen: 35-37
If one cannot find an al Qaeda operative in publicly available sources in Denmark, the researcher could assume there is no al Qaeda network in Denmark.	If one cannot find an al Qaeda operative in the U.S. in publicly available sources, the researcher could assume there is no al Qaeda network.

Anmerkungen

This sentence is the almost seamless continuation of the section which Nm began to copy on pages 33 and 34 of his thesis.

[23.] Nm/Fragment 038 04

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 38, Zeilen: 4-23	Quelle: Koelle et al 2006 Seite(n): 2 (internet version), Zeilen: right column 3-26
1.5.2 Homogeneous Link Types Social network analysis does not fully report the need to characterize different types of links. A link in a social network graph can represent a variety of concepts and relationships. For example: an evaluation (A likes B or A respects B), behavioural interaction, similarity, association, affiliation, physical connection, formal relations, (such as authority), and biological relations (Wasserman & Faust, 1994). Links can be of different types. Link types can also indicate the strength of a particular concept. For example, link type "friendship" can be further classified four subtypes: "No contact", "small talk and coffee", "exchange of favours", and "close ties" (Heran, F., 1987). While traditional graph based algorithms used for SNA may incorporate analysis of different node and link types. However, they incline to be homogeneous within a network (i.e., considering a single node or link type per analysis), rather than being heterogeneous within a network (i.e., multiple link and node types). Further, graph based algorithms do not typically consider attributes on links or nodes.	**2.2 HOMOGENEOUS NODE AND LINK TYPES** Social network analysis does not fully address the need to characterize different types of relationships. A social network graph can represent a variety of concepts through links, such as evaluation (A likes B, A respects B), behavioral interaction, transfers of material resources, association, affiliation, movement between places or statuses, physical connection, formal relations (such as authority), and biological relations (Wasserman & Faust, 1994). Different links types can also indicate the strength of a particular concept. For example, one social network construction study offered subjects four choices to identify the intensity of their friendships: "No contact", "small talk and coffee", "exchange of favors", and "close ties" (Heran, 1987). While traditional graph-theoretic algorithms used for SNA may incorporate analysis of different node and link types, they tend to be homogeneous within a network (i.e., considering a single node or link type per analysis), rather than being heterogeneous within a network (i.e., multiple link and node types). Further, graph-theortic algorithms do not typically consider attributes on links or nodes [...]

Anmerkungen

Highly similar, with the source not being mentioned anywhere in Nm's thesis.

[24.] Nm/Fragment 038 27

KomplettPlagiat

Untersuchte Arbeit: Seite: 38, Zeilen: 27-30	Quelle: Westphal and Blaxton 1998 Seite(n): 201, Zeilen: 2-5
One of the variations is link analysis. It is the process of building up networks of interconnected objects through relationships in order to expose patterns and trends. Link analysis uses item-to-item associations to generate networks of interactions [and connections from defined datasets.]	Link analysis is the process of building up networks of interconnected objects through relationships in order to expose patterns and trends. Link analysis uses item-to item associations to generate networks of interactions and connections from defined data sets.

Farbig

Anmerkungen

Keine Kennzeichnung als Zitat, kein Hinweis auf die Quelle

[25.] Nm/Fragment 039 01

Verschleierung

Untersuchte Arbeit: Seite: 39, Zeilen: 1-20	Quelle: Westphal and Blaxton 1998 Seite(n): 201, Zeilen: 3-20
[Link analysis uses item-to-item associations to generate networks of interactions] and connections from defined datasets. The diagrams of link analysis have a variety of names ranging from entity-relationship diagrams and connected networks to nodes-and-links and directed graphs. The methods of link analysis add dimensions to an analysis that the other form of visualization do not support. By explicitly representing relationships among objects, an entirely different perspective on how the data can be analysed and the types of patterns that can be discovered. Link analysis systems were initially used primarily in investigative world (e.g., law enforcement), but they have recently made significant inroads into a variety of commercial applications. One potential drawback of link analysis is that the aggregate number of data records that can be presented in most diagrams is somewhat limited, as compared to other visualization paradigms. As a result, the analyses tend to focus on verifying subsets of large datasets. Nevertheless, link analysis provides a powerful means of performing visual data mining, particularly if we know how to take advantage of layout options, filter assessments, and presentation formats. The link analysis systems allow the identification of patterns, emerging groups, and generational connections quickly.	Link analysis uses item-to item associations to generate networks of interactions and connections from defined data sets. Link analysis diagrams have a variety of names ranging from entity-relationship diagrams and connected networks to nodes-and-links and directed graphs. Link analysis methods let you add dimensions to an analysis that the other forms of visualization do not support. By explicitly representing relationships among objects you gain an entirely different perspective on how the data can be analyzed and the types of patterns that can be discovered. Link analysis systems were initially used primarily in the investigative world (e.g., law enforcement) but they have recently made significant inroads into a wide variety of commercial applications. One potential drawback of link analysis is that the aggregate number of data records that can be presented in most diagrams is somewhat limited, as compared to the other visualization paradigms. As a result, the analyses tend to focus on verifying subsets of large data sets. Nevertheless, link analysis provides a powerful means of performing visual data mining, particularly if you know how to take advantage of layout options, filter assessments, and presentation formats. Used properly, link analysis systems allow you to identify patterns, emerging groups, and generational connections quickly.

Farbig

Anmerkungen

Only the slightest of changes, it is not marked as a citation, and no source is given

[26.] Nm/Fragment 040 01

Verschleierung

Untersuchte Arbeit: Seite: 40, Zeilen: 1-9	Quelle: Carley 2006 Seite(n): 53, Zeilen: 31-37
In addition to the previous discussion, link analysis is basically a descriptive approach for exploring data in order to identify relationship among values in the database. In this approach, the user lays out graphically; the links between various entities; such as people, resources, and locations. A key limitation of this approach is that it is a primary a tool for visualization and organization. There are no analytic metrics attached. As such, there are no procedures for analyzing the data estimating who or what should be targeted to achieve what effects, or for estimating [...]	Visual link analysis is basically a descriptive approach to exploring data in order to identify relationships among values in a database. In this approach, the user lays out graphically the links between various entities such as people, resources, and locations. A key limitation of this approach is that it is primarily a tool for visualization and organization. There are no analytic metrics or attached. As such, there are no procedures for analyzing the data and estimating what data is missing, who or what should be targeted to achieve what effects, or for estimating [...]

Farbig

Anmerkungen

nothing is marked as a citation, source is not given.

[27.] Nm/Fragment 040 22

Verschleierung

Untersuchte Arbeit: Seite: 40, Zeilen: 22-32	Quelle: Ressler 2006 Seite(n): 4, 5, Zeilen: p.4,3-6.8-11 and p.5,32-33
After 9/11 attacks, the academic world has increased the attention paid to the analysis of terrorist networks because of public interest. Network analysis of terrorist organizations is divided into two groups: data collectors and data modelers: Data collection is difficult for network analysis because it is hard to create a complete network (as already discussed). It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on the members, and governments rarely allow researchers to use their intelligence data. There has been limited work in the field of complex modeling of terrorist networks.	[p. 4] Since the winter of 2001, the academic world has increased the attention paid to the social network analysis of terrorism as a result of public interest and new grant money. [FN 15] Network analysis of terrorist organizations continues to grow and can be divided into two groups: the data collectors and the modelers. [...] Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. [p. 5] There has been limited work in the field of complex modeling of terrorist networks outside the work of Kathleen Carley and her associates.

Farbig

Anmerkungen

The paragraph from line 26 to 30 can already be found on page 33 Nm/Fragment_033_15 of Nm's thesis. Comparing these two paragraphs, one can see directly how Nm tries to camouflage his copying

[28.] Nm/Fragment 041 01

Verschleierung

Untersuchte Arbeit: Seite: 41, Zeilen: 1-6	Quelle: Ressler 2006 Seite(n): 6, Zeilen: 1-6
[A common problem for the modelers is the] issue of data. Any academic work is only as good as the data, no matter the type of advanced methods used. It is, well known fact that modelers often do not have the best data and they do not have access to classified data. Many of the models are created without data or with incomplete data. The implication of this is that the results can be potentially misleading.	A common problem for the modelers is the issue of data. Any academic work is only as good as the data, no matter the type of advanced methods used. Modelers often do not have the best data, as they have not collected individual biographies (like Sageman) and do not have access to classified data. Many of the models are created data-free or without complete data, yet do not fully consider human and data limitations. The implication of this is that the results can be potentially misleading, [...]

Farbig

Anmerkungen

Continued from last page: no reference to the source is given.

[29.] Nm/Fragment 041 08

Verschleierung

Untersuchte Arbeit: Seite: 41, Zeilen: 8-15	Quelle: Saxena et al. 2004 Seite(n): 85, Zeilen: 6-12	Farbig
The increase of number of terrorism incidents in recent years has increased the feeling of insecurity and danger in many countries. In this regard, classified information with government agencies is not available to the public or academic research institutions. However, the Internet revolution has opened up a new ways by providing huge volume of information on these incidents. Such information in open domain can be a used to create a knowledge base which, after proper cleaning could be useful for intelligence analysis.	The increase in violent terrorist incidents, in recent years, has heightened the feeling of insecurity in many countries. In this regard, privileged information with government agencies is not available to the public or academic research institutes. However, the IT revolution has opened up a growing volume of information on these incidents. This information in the open domain can be a valuable resource in creating a data base which, after proper capture, cleaning and classification could be useful in strategic analysis	

Anmerkungen

The source is not mentioned in the entire thesis.

[30.] Nm/Fragment 041 28

Verschleierung

Untersuchte Arbeit: Seite: 41, Zeilen: 28-31	Quelle: Visualcomplexity 2006 Seite(n): 1, Zeilen: -	Farbig
This website is database of open source information about the Al Qaeda terrorist network, developed as a research project of the FMS Advanced Systems Group. The goal of creating this database is to apply new technologies and software engineering [approaches to open source intelligence while providing researchers and analysts with information about Al Qaeda.]	TrackingTheThreat.com is database of open source information about the Al Qaeda terrorist network, developed as a research project of the FMS Advanced Systems Group. The goal is to apply new technologies and software engineering approaches to open source intelligence while providing researchers and analysts with information about Al Qaeda.	

Anmerkungen

the source is not given

[31.] Nm/Fragment 042 01

Verschleierung

Untersuchte Arbeit: Seite: 42, Zeilen: 1-2	Quelle: Visualcomplexity 2006 Seite(n): 1, Zeilen: -	Farbig
[The goal of creating this database is to apply new technologies and software engineering] approaches to open source intelligence while providing researchers and analysts with information about Al Qaeda.	The goal is to apply new technologies and software engineering approaches to open source intelligence while providing researchers and analysts with information about Al Qaeda.	

Anmerkungen

Source is not given. Copied text starts on the previous page.

[32.] Nm/Fragment 042 03

Verschleierung

Untersuchte Arbeit: Seite: 42, Zeilen: 3-9	Quelle: TrackingTheThreat.com 2006 Seite(n): 1 (internet version), Zeilen: 26-30
In order to create a huge database, FMS Advanced Systems Group collected real-world data—information about the people, places, events, connections, and other metadata about Al Qaeda in general, and 9/11 in particular. Several months of research using opensource materials, such as articles on the web, books, magazines, and other information yielded Al Qaeda dataset—a large collection of structured entity and relationship information.	In order to test the prototype system, we needed real-world data—information about the people, places, events, connections, and other metadata about Al Qaeda in general, and 9/11 in particular. Several months of research using open-source materials, such as articles on the web, books, magazines, and other information yielded our initial Al Qaeda dataset—a large collection of structured entity and relationship information.

Farbig

Anmerkungen

not marked as a citation, no source given

[33.] Nm/Fragment 042 12

Verschleierung

Untersuchte Arbeit: Seite: 42, Zeilen: 12-18	Quelle: Saxena et al. 2004 Seite(n): 85, Zeilen: 17-21
Terrorist and criminal organizations, generally organize themselves as secret networks with distributed work share. It is difficult to obtain information in the open domain on their membership, links and management or confirm the validity of such information. Still then, due to the need of publicity for the terrorists, for their cause, the open source information becomes relevant in exploring terrorist networks.	Terrorist and criminal organisations, generally, organise themselves as secret networks with distributed work share. It is not easy to obtain confirmed information in the open domain on their membership, ties and management. However, terrorists need the oxygen of publicity for their 'cause'; and, hence, open source information [EN 1] becomes relevant in exploring such networks.

Farbig

Anmerkungen

No source is given for this short paragraph.

[34.] Nm/Fragment 044 18

KomplettPlagiat

Untersuchte Arbeit: Seite: 44, Zeilen: 18-22	Quelle: Ressler 2006 Seite(n): 6, Zeilen: 8-11
It would be quite difficult to model the network structure and evolution of Al Qaeda since many of the organizations that claim ties to Al Qaeda are lying and do not actually have those ties. It can be quite difficult differentiating these groups from other, truly loosely affiliated groups.	For example, it would be quite difficult to model the network structure and evolution of al Qaeda since many of the organizations that claim ties to al Qaeda are lying and do not actually have those ties. It can be quite difficult differentiating these groups from other, truly loosely affiliated groups.

Farbig

Anmerkungen

One more paragraph that Nm has taken from Ressler (2006) leaving it unchanged, not marking it as a citation and without referencing the source.

[35.] Nm/Fragment 044 23

Verschleierung

Untersuchte Arbeit: Seite: 44, Zeilen: 23-30	Quelle: Hamill_2006 Seite(n): 3, Zeilen: 17-26	Farbig
1.8. PROBLEM DEFINITION	1.2 Problem Definition	
The primary objective of this research is to expand data mining research, sociological, and behavioural theory relevant to the study of terrorist networks, thereby providing theoretical foundations for new and useful methodologies to analyze terrorist networks. For the purposes of this research, terrorist networks are those trying to hide their structures or are unwilling to provide evidence regarding their actions (Sparrow, 1991; Van Meter, 2002).	The overarching objective of this research is to expand operations research, sociological, and behavioral theory relevant to the study of social networks, thereby providing theoretical foundations for new and useful methodologies to analyze noncooperative organizations. [...] For the purposes of this research, non-cooperative organizations are those trying to hide their structures or are unwilling to provide information regarding their operations; [...] [cf., Sparrow, 1991; van Meter, 2002].	

Anmerkungen

The original source Hamill (2006) is not given.

The publication Van Meter (2002) is not listed in the bibliography.

[36.] Nm/Fragment 045 01

Verschleierung

Untersuchte Arbeit: Seite: 45, Zeilen: 1-16	Quelle: Carley 2006 Seite(n): 51-52, Zeilen: p.51,14.15-20 - p.52,1-5	Farbig
Terrorist networks are so often challenging to reason about and manage. These networks differ on many dimensions. For examples, terrorist networks range in complexity and lethalness of the weaponries they use, the level and source of their fiscal support, their core organizational structure, and their linking to organized crime, the local police and other terrorist or rebellious groups. Despite these differences, in general, these groups rely on communication groups, with and without advanced information technology, to employ, organize, design, direct, and perform terrorist attacks. As such targeting mechanisms aimed at information, channels, and actors can be used to classify those relations and nodes that are actual targets for disrupting the organizational movement or interrelation of these terrorist networks. Investigative data mining provides a means for detecting such targets and assessing the impact of different courses of action on the terrorist networks.	[page 51] Covert networks are often difficult to reason about and manage. [...] These groups[FN 1] vary on many dimensions. For example, terrorist groups range in the sophistication and deadliness of the weapons they use, the level and source of their financial support, their internal organizational structure, and their connection to organized crime, the local police and other terrorist or insurgent groups. Despite these differences, in general, these groups rely on communication networks, with and without advanced information technology, to recruit, organize, plan, direct, and [page 52] execute terrorist acts. As such, targeting mechanisms aimed at information, channels, and actors can be used to identify those links and nodes that are effective targets for destabilizing the organizational activity or cohesion of these covert networks. Dynamic network analysis provides a means for identifying such targets and assessing the impact of alternate courses of action on these covert networks.	

Anmerkungen

Only small bits and pieces have been exchanged; otherwise the text has been left more or less intact. No reference to the source is given.

[37.] Nm/Fragment 045 18

Verschleierung

Untersuchte Arbeit: Seite: 45, Zeilen: 18-23	Quelle: Koschade 2005 Seite(n): 2 and 3, Zeilen: p. 2,6-8 and p. 3,31-35
IDM offers the ability to map a covert cell, and to measure the specific structural criteria of such a cell. This framework aims to connect the dots between individuals and "map and measure complex, covert, human groups and organisations". 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".	[p. 2] 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. [p. 3] This framework aims to connect the dots between individuals and "map and measure complex, sometimes covert, human groups and organisations". [EN 8] The method focuses on uncovering the patterning of people's interaction, [EN 9] and correctly interpreting these networks assists "in predicting behaviour and decision-making within the network". [EN 10] --- [EN 8] Krebs, V. (2002) "Mapping Networks of Terrorist Cells", Connections, Vol. 24, 3, pp. 43-52. [EN 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. [EN 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.

Farbig

Anmerkungen

While the original text gives references for each sentence, Nm has only left the quotation marks and gives neither the original sources nor the source of this section.

Furthermore Nm uses this text in his thesis for the second time, the other is Nm/Fragment_025_22

[38.] Nm/Fragment 046 09

Verschleierung

Untersuchte Arbeit: Seite: 46, Zeilen: 9-19	Quelle: Hamill_2006 Seite(n): 9, Zeilen: 6ff
1.9. RESEARCH OBJECTIVES The primary objective of this research is to develop the underlying theory and allied methodology used to produce and analyze terrorist networks and proposes mathematical methods for destabilizing these adversaries. The specific objectives of this research include to: ▪ Develop a new centrality-like measure, via extensions of several others in use to screen networks for potential actors of interest. The theoretical bases that make this measure more amenable to terrorist networks, advantages over other measures are presented.	1.4 Research Objectives The primary objective of this research is to develop the underlying theory and associated methodology used to generate and analyze courses of action that may be applied to networks of non-cooperative individuals. [...] Specific objectives of this research include: 1. Develop a new centrality-like measure, via extensions of several others in use, to screen networks for potential actors of interest. The theoretical bases that [page 10] make this measure more amenable to non-cooperative networks, advantages, and computational challenges are presented.

Farbig

Anmerkungen

no source given: even the research objectives are partially copied.

[39.] Nm/Fragment 047 09

Verschleierung

Untersuchte Arbeit: Seite: 47, Zeilen: 9-15	Quelle: Hamill 2006 Seite(n): 11, Zeilen: 7-12
• Combine the most promising techniques into a prototype tool-set, developed in Java, for intelligence analysis. **1.10. DISSERTATION OVERVIEW** The organization of this dissertation document is as follows. Chapter 2 presents the background literature relevant to the problem areas and builds the case for the contribution objectives described above. Chapter 3 [...]	7. Combine the most promising techniques into a prototype tool-set, developed in MATLAB, for intelligence analysis use by the sponsoring organizations. **1.5 Dissertation Overview** The organization of this dissertation document is as follows. Chapter II presents the literature relevant to the problem areas and builds the case for the contribution objectives described above. Chapter III [...]

Farbig

Anmerkungen

no source given, nothing marked as a citation

[40.] Nm/Fragment 047 22

Verschleierung

Untersuchte Arbeit: Seite: 47, Zeilen: 22-25	Quelle: Hamill 2006 Seite(n): 11, Zeilen: 19-22
Chapter 5 explores the nuances of persuasion and power theory in order to estimate hidden hierarchy from nonhierarchical / horizontal terrorist networks. Some case studies are provided for illustrative purposes throughout the document.	Chapter VII explores the nuances of persuasion and power theory in order to estimate gains and losses of information or influence as a function of sender-receiver interactions. Although smaller examples are provided for illustrative purposes throughout the document. [...]

Farbig

Anmerkungen

continues the using of bits and pieces from Hamill's "Dissertation Overview"; no reference given

[41.] Nm/Fragment 048 05

Verschleierung

Untersuchte Arbeit: Seite: 48, Zeilen: 5-6	Quelle: Hamill 2006 Seite(n): 11, Zeilen: 24-25
Chapter 9 provides an overall, general conclusions as well as recommendations for future research.	Chapter IX provides overall, general conclusions as well as recommendations for future research.

Farbig

Anmerkungen

Finishes the copying of bits and pieces from Hamill's (2006) Section 1.5.

[42.] Nm/Fragment 049 04

BauernOpfer

Untersuchte Arbeit: **Seite: 49, Zeilen: 3-28**	**Quelle: DCSINT_2005** **Seite(n): 2-10, Zeilen: 6-14, 15-24**

Farbig

2.1 OVERVIEW[FN 9]

"Terrorism is a psychological act that communicates through the medium of violence or the threat of violence" (Gunaratna, R., 2000). Terrorist strategies will be aimed at publicly causing damage to symbols or inspiring horror. Timing, location, and method of attacks accommodate media dissemination and ensure "newsworthiness" to maximize impact.

A terrorist operation will often have the goal of manipulating popular perceptions, and will achieve this by controlling or dictating media coverage. This control need not be evident, as terrorists analyze and exploit the dynamics of major media outlets and the pressure of the "news cycle" (Hoffman, B., 1998). The bombing of commuter trains in Madrid is one example of such theory. The true cause behind Madrid bombing is not determined yet. However, one view is that terrorists who specifically planned to influence the political process in Spain conducted the attacks. They believed that the public would feel the current government responsible, as the large percentage of population was against the involvement of Spanish forces in Iraq war. The attacks occurred during the morning rush hour just three days prior to the national elections. Timing the attack played a vital role in maximizing casualties on the trains (killing 191 people and injuring more than 1800), and immediate world over news coverage. Although, there are fair chances of coincidence, but an anti-war Socialist prime minister was elected in the following election who quickly withdrew Spain's military forces from Iraq.

[FN 9] Some parts of this Sections are taken from "A Military Guide to Terrorism in 21st Century"

[FN 110]

[...]

Terrorism is a psychological act that communicates through the medium of violence or the threat of violence. Terrorist strategies will be aimed at publicly causing damage to symbols or inspiring fear. Timing, location, and method of attacks accommodate media dissemination and ensure "newsworthiness" to maximize impact.

A terrorist operation will often have the goal of manipulating popular perceptions, and will achieve this by controlling or dictating media coverage. This control need not be overt, as terrorists analyze and exploit the dynamics of major media outlets and the pressure of the "news cycle."[FN 111] A terrorist attack that appears to follow this concept was the bombing of commuter trains in Madrid, Spain in March 2004. [...] One view is that Islamic terrorists who specifically planned to influence the political process in Spain conducted the attacks. They believed that the large percentage of the Spanish population opposed the war in Iraq and would feel that the current government was responsible for the bombings, and would therefore vote for the opposition. The attacks occurred during morning rush hour just three days prior to national elections. The timing facilitated maximum casualties on the trains (killing 191 people and injuring more than 1800), plus immediate news coverage throughout the world of the carnage resulting from this terrorist attack. Although it cannot definitively be linked to the bombings, an anti-war Socialist prime minister was elected who quickly withdrew Spain's military forces from Iraq.

[FN 110] Rohan Gunaratna, "Suicide Terrorism: a Global Threat," *Jane's Intelligence Review* (20 October 2000): 1-7; available from http://www.janes.com/security /international_security/ news/usscole /jir001020_1_n.shtml; Internet; accessed 7 September 2002.

[FN 111] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 136-142.

Anmerkungen

The footnote mentions the source (however without telling the version of the document, nor any bibliographical details). This is done in a way that makes not clear to the reader, what exactly is taken from the source.

[43.] Nm/Fragment 050 01

BauernOpfer

Untersuchte Arbeit: Seite: 50, Zeilen: 1-21	Quelle: DCSINT_2005 Seite(n): 2-10, Zeilen: p.2-10,25-38 - p.2-11,1-2

Farbig

[A] massively launched attack against a target which will not yield enough media coverage is not viable for terrorists as compared to a small attack against a “media accessible” target. However, with the spread of the global media, many locations have potential to become attractive targets that would not have been considered thirty or forty years ago.

The 1998 bombings of the American embassies in Kenya and Tanzania are an example showing how these two relatively unimportant posts created a global sensation because of the modern media coverage. Forty years ago it would have taken days for the international news media to get photographs and relevant text from these locations, making them much less attractive targets in those days. However, with modern technology, it was possible to provide immediate broadcast coverage of the incident. Since the religious justification was the known cause behind the attacks, but still the worldwide coverage of these attacks made it possible for these terrorists to pose as champions of a cause, even in the absence of any effective work at the grassroots level of society (Kepel, G., 2002). The September 11, 2001 bombing of the World Trade Center in New York City was observed live on television by millions of people

[p 2-10] In considering possible terrorist targets, recognize that a massively destructive attack launched against a target that cannot or will not attract sufficient media coverage to impact the target audience is not a viable target for terrorists. A small attack against a “media accessible” target is better than a larger one of less publicity. However, the spread of the global media makes many locations attractive targets that would not have been remotely considered thirty or forty years ago. The 1998 bombings of the American embassies in Kenya and Tanzania illustrate how these two relatively unimportant posts created a global sensation because of the media coverage. Forty years ago it would have taken days for the international news media to get still photographs and some text from these locations, making them much less attractive targets. However, with today’s modern technology, media reporters were able to provide immediate broadcast coverage of the bombings. Since the Islamist factions that conducted the attacks used religious justifications for their actions, the worldwide coverage of these attacks made it possible for these terrorists to pose as champions of a cause, even in the absence of any effective work at the grassroots level of society. [FN 112] The September 11, 2001 bombing of

---

[FN 112] Gilles Kepel, *Jihad: The Trail of Political Islam* (Cambridge: The Belknap Press of Harvard University Press): 320.

[p. 2-11]

the World Trade Center in New York City was observed by millions of people worldwide on live television as the successive attacks occurred and sensational mass destruction followed.

Anmerkungen

continued from the previous page.

Note FN 9 from the previous page: "Some parts of this Sections are taken from 'A Military Guide to Terrorism in 21st Century'"

[44.] Nm/Fragment 050 22

BauernOpfer

Untersuchte Arbeit: Seite: 50, Zeilen: 22-30	Quelle: Bedi 2005 Seite(n): 6, Zeilen: 29-34

Farbig

2.2 TYPES OF TERRORISTS

Bedi Rohan (2005) investigated four types of terrorists:

1) Unknown persons: The person who is inspired by a cause and wants to become a terrorist, but due to absence of an experienced counsellor is likely to fall in this type of terrorists. Such persons often get caught early because of the sheer incompetence of their schemes. These can also behave like lone operators in specific situations.

2) New terrorists: The people who are indoctrinated at some [religious school preaching extremism, who commit an act of terrorism just or shortly after being brainwashed and trained.]

Four Types of Terrorists

1) Unknown persons (who could also be lone operators) who are inspired by a cause and want to become terrorists but can’t find a more experienced mentor. Such persons often get caught early because of the sheer incompetence of their schemes.

2) New terrorists indoctrinated at some religious school preaching extremism who commit an act shortly after being brainwashed and trained.

Anmerkungen

Even though the reference is given, the reader is left in the dark about how close to the original text Nm stays. Literally copied text is not marked as such.

Also refer to the next page Nm/Fragment_051_01, where more text is copied word for word.

[45.] Nm/Fragment 051 01

BauernOpfer

Untersuchte Arbeit: **Seite: 51, Zeilen: 1-2, 4-31**	**Quelle: Bedi 2005** **Seite(n): 6-7, Zeilen: p.6,33-42; p.7:1-11**
[2) New terrorists: The people who are indoctrinated at some] religious school preaching extremism, who commit an act of terrorism just or shortly after being brainwashed and trained. [...] The persons who get indoctrinated through the internet and somehow find themselves a mentor, or self-train using the urban warfare training that Al Qaeda has made readily available on the internet can be classified in this terrorist group.	[p. 6] 2) New terrorists indoctrinated at some religious school preaching extremism who commit an act shortly after being brainwashed and trained. There are also persons who get indoctrinated through the internet and somehow find themselves a mentor and self-train using the urban-warfare training that al-Qaeda has made readily available on the internet.
3) Sleepers: People in touch through family and friends' connections with experienced terrorists, who act as their mentors and train them group wise. Sometimes sleepers are small groups embedded in the migrant settler community that due to incomplete integration into the host society may have hidden cells engaged in terrorist and criminal operations. Even the presence of mentor is not necessary in such situations. The police does not have enough proof (if there is some) to lock them up or list them as wanted publicity, albeit they may be monitoring some of them.	3) "Sleepers" in touch through family and friends' connections with experienced terrorists who act as their mentors and train them in small groups. Sometimes sleepers are small groups embedded in the migrant settler community that due to incomplete integration into the host society may have hidden cells engaged in terrorist and criminal activities with or without a mentor. The police have insufficient proof (if at all) to lock them up/ put them on a public black-list albeit they may be monitoring some of them.
4) Known hard-core terrorists: People on the most wanted list of the FBI and other intelligence or law enforcement agencies.	[p. 7] 4) Known hardcore terrorists on the most wanted list of the FBI and other black-lists.
With the focus on anti-terrorism in the West, the first type is increasingly being foiled at an early stage and with limited damage. However, the second category of terrorists is difficult to spot. For example, the London July 2005 bombers included a young Pakistani boy belonging to a good family, who unfortunately was influenced by some person(s) he met at a religious school. Or, the other example is of Mohammad Momin Khawaja, who was indoctrinated through the Internet and was arrested by the Canadian police after collaborating with the UK in March 2004, in connection with a large UK plot. He was a Canadian citizen, a contractual software operator in the Canadian Foreign Affairs Department, earning a decent income. He never got any formal training, however he was probably trained by Al Qaeda mentor [using the Internet.]	With the focus on anti-terrorism in the West, the first category is increasingly being foiled at an early stage with limited damage. The second category of terrorists, for example, the recent London July 2005 bombers included a young Pakistani boy from a good family who unfortunately got swayed under the influence of some person(s) he met at a religious school. Or, the example of Mohammad Momin Khawaja indoctrinated through the internet, who was arrested by the Canadian police collaborating with the UK in March 2004, in connection with a large UK plot. He was a Canadian citizen of Pakistani origin, a contract computer software operator with the Canadian Foreign Affairs Department earning a decent income. He never got any formal training albeit he did manage to get himself an al-Qaeda mentor and probably trained himself using the internet.

Anmerkungen

continues from the previous page. After the first three paragraphs of this page it is not clear anymore that the source is still Bedi (2005), but also in the first three paragraphs there is text copied word-for-word without making that clear to the reader.

[46.] Nm/Fragment 052 01

Verschleierung

Untersuchte Arbeit: Seite: 52, Zeilen: 1-17	Quelle: Bedi 2005 Seite(n): 7, Zeilen: 10-14, 16-23
[He never got any formal training, however he was probably trained by Al Qaeda mentor] using the Internet. Such cases are naturally tough to spot on, no matter how detailed any database is.	He never got any formal training albeit he did manage to get himself an al-Qaeda mentor and probably trained himself using the internet. Such cases are naturally tough to spot on any database.
The third category of terrorists are for example, the Madrid bombers who may not have been on the US black-list at the time of Madrid Bombing, However, they are said to had ties to a ring of petty criminals that smuggled drugs and others who were involved in bank ATM fraud and robbery. Still, the masterminds were trained by Al Qaeda.	The third category of terrorists are for example, the Madrid bombers who may not have been on the US OFAC black-list [...]. The Madrid Bombers had ties to a ring of petty criminals that smuggled drugs and others who were involved in bank ATM fraud and robbery. The masterminds were al-Qaeda trained.
The fourth category is obviously the easiest to spot provided that identity theft and impersonations are detectable. The biggest problem with this category is that they would avoid completing transactions in their true names, that is, they would use identity theft to help them conceal their identities. People in this category include individuals who may have been to the Al Qaeda training camps in Afghanistan prior to 2001. For example, as many as 3,000 British born or based people are thought to have been trained in the camps and may since have trained others.	The fourth category is obviously the easiest to spot albeit they would avoid doing transactions in their names ie, they would use identity theft to help them conceal their identities. People in this category include individuals who had been to the al-Qaeda training camps in Afghanistan prior to 2001. For example, as many as 3,000 British born or based people are thought to have been trained in the camps and may since have trained others.

Farbig

Anmerkungen

continued from previous page. The source is given two pages further up, the reader would never assume that he is reading Bedi here instead of Nm.

[47.] Nm/Fragment 052 18

BauernOpfer

Untersuchte Arbeit: Seite: 52, Zeilen: 18-29	Quelle: Shelley 2002 Seite(n): 1, Zeilen: 4-11
The problems of organized crime and terrorism were often considered separate phenomena prior to September 11. The security studies committee, the military and some parts of law enforcement increasingly viewed terrorism and transnational crime as distinct strategic threats. Seminars would discuss the emerging threat of transnational crime or terrorism but the important links between the two were rarely made (Shelley I. L., 2002).	The problems of organized crime and terrorism were often considered separate phenomena prior to September 11th. The security studies committee, the military and parts of law enforcement increasingly viewed terrorism and transnational crime as strategic threats. But these problems were often seen as distinct. Seminars would discuss the emerging threat of transnational crime or terrorism but the important links between the two were rarely made.
2.3 TERRORISM AND ORGANIZED CRIME The 9/11 attacks have changed the strategic thinking in this area. Terrorism and transnational crime are now considered as central threats to our national and international security. But, still more needs to be understood about the inter-linkage between the two [phenomena.]	September 11th has changed the strategic thinking in this area. Terrorism and transnational crime are now central threats to our national and international security. Yet more needs to be understood about the links between these two phenomena.

Farbig

Anmerkungen

Although the reference has been given by Nm the reader does not expect the paragraphs to be nearly identical since nothing has been marked as a citation.

[48.] Nm/Fragment 053 01

BauernOpfer

Untersuchte Arbeit: Seite: 53, Zeilen: 1-20	Quelle: Shelley 2002 Seite(n): 1 (internet version), Zeilen: 11-13, 15-27
Mass media reports many illustrations of crime and terrorism link in Western Europe and the United States. However, much less has been written on this subject in the Pacific context. Illustrations of the links between organized crime and terrorism are the follows (Shelley I. L., 2002):	Many illustrations of the crime and terrorism link in Western Europe and the United States have appeared in the mass media. Much less has been written on this subject in the Pacific context. [...] Illustrations of the links between organized crime and terrorism are the following:
1) Terrorists engage in organized crime activity to raise funds and strengthen their financial position.	1) Terrorists engage in organized crime activity to support themselves financially
2) Both terrorists and organized crime groups often operate in form of networks. Sometimes these structures intersect, and thus terrorists can hide themselves among transnational criminal organizations	2) Organized crime groups and terrorists often operate on network structures and these structures sometimes intersect, terrorists can hide themselves among transnational criminal organizations
3) Both organized crime groups and terrorists operate in similar areas. The areas with weak governmental controls and enforcement of laws, and open borders are usually considered in this regard.	3) Both organized crime group and terrorists operate in areas with little governmental controls, weak enforcement of laws and open borders
4) Both organized criminals and terrorists corrupt or use corrupt local officials to achieve their objectives	4) Both organized criminals and terrorists corrupt local officials to achieve their objectives
5) Organized crime and terrorists launder their money, often using the same methods and often the same operators to move their funds	5) Organized crime groups and terrorists often use similar means to communicate-exploiting modem technology
6) Organized crime groups and terrorists often use similar means to communicate.	6) Organized crime and terrorists launder their money, often using the same methods and often the same operators to move their funds

Farbig

Anmerkungen

Nm names his source as "Shelley I. L., 2002" - but the extent of the copying, especially with much word-for-word copying, is not made clear.

[49.] Nm/Fragment 053 21

KomplettPlagiat

Untersuchte Arbeit: Seite: 53, Zeilen: 21-30	Quelle: Shelley 2002 Seite(n): 2 (internet version), Zeilen: 26-33
Transnational crime groups often operate on a network structure. The network structure is not unique to this group but characterizes many other terrorist groups and many of the new transnational organized crime groups. Unlike the top-down- hierarchical structure of a mafia-type organization, newer organized crime groups such as Russian-speaking groups and terrorist groups such as the Al Qaeda function as networks. It gives organizational flexibility, reduces the possibility of penetration and provides greater efficiency. These structures make it more difficult to identify leaders. The newer criminal groups and leading terrorist [organizations resemble more modern legitimate business structures than the older corporations like Ford and the steel industry.]	Transnational crime groups often operate on a network structure. The network structure is not unique to this group but characterizes many other terrorist groups and many of the new transnational organized crime groups. Unlike the top-down-hierarchical structure of a mafia-type organization, newer organized crime groups such as Russian-speaking groups and terrorist groups such as the Al Qaeda function as networks. It gives organizational flexibility, reduces the possibility of penetration and provides greater efficiency. These structures make it more difficult to identify leaders. The newer criminal groups and leading terrorist organizations resemble more modern legitimate business structures than the older corporations like Ford and the steel industry.

Farbig

Anmerkungen

Copy of the original - not marked as a citation. The source has been mentioned with respect to the foregoing list.

[50.] Nm/Fragment 054 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 54, Zeilen: 1-12	Quelle: Shelley 2002 Seite(n): 2 (internet version), Zeilen: 32-40
[The newer criminal groups and leading terrorist] organizations resemble more modern legitimate business structures than the older corporations like Ford and the steel industry.	The newer criminal groups and leading terrorist organizations resemble more modern legitimate business structures than the older corporations like Ford and the steel industry.
Organized crime networks are often of the same nationality, though they form alliances with other foreign crime groups to conduct their activities. In contrast, the networks of groups such as Al Qaeda are considered themselves transnational. They can unite individuals from the Middle East with those in the Far East. Likewise, the organized crime groups in the Russian Far East work with North and South Koreans, Japanese, Chinese and Vietnamese among others. The networks are not usually affiliated with any particular state. They are non-state actors striking at the citizens of a state or different states.	Organized crime group networks are often of the same nationality, though they form alliances with other crime groups to conduct their activities. In contrast, the networks of groups such as Al Qaeda are themselves transnational. They can unite individuals from the Middle East with those in the Far East. Likewise, the organized crime groups from the Russian Far East work with North and South Koreans, Japanese, Chinese and Vietnamese among others. The networks are not affiliated with any particular state. They are non-state actors striking at the citizens of a state, states or different states.

Farbig

Anmerkungen

Continues the copying process from the previous page.

[51.] Nm/Fragment 054 13

Verschleierung

Untersuchte Arbeit: Seite: 54, Zeilen: 13-23	Quelle: Shelley 2002 Seite(n): 4 (internet version), Zeilen: 9-15
Terrorists, like transnational organized crime, use the information technology to maximize the effectiveness of their operations. For example the use of cellular and satellite telephones, the Internet, email and chat rooms are being used by them. The communication is facilitated with encryption and stenography (hiding messages within other messages). The anonymous interactive features of the Internet are used to evade detection. Whereas, organized criminals run gambling on the Internet, terrorists solicit funds through websites for charities that fund terrorist groups. International bank transfers and other fund movement technologies are also used by terrorists.	Terrorists, like transnational organized crime, exploit information technology to maximize the effectiveness of their operations. They use cellular and satellite telephones, the Internet, email and chat rooms. They code their messages through encryption and steganography (hiding messages within other messages). They exploit the anonymyzer features of the Internet to evade detection. The Internet is a tool for perpetration of their crimes. Whereas, organized criminals run gambling on the Internet, terrorists solicit funds through websites for charities that fund terrorist groups. International fund movements are facilitated by information technology.

Farbig

Anmerkungen

still copying from the same source - but this time with a mistake that confuses the meaning: "steganography" becomes "stenography"

[52.] Nm/Fragment 054 23

Verschleierung

Untersuchte Arbeit: Seite: 54, Zeilen: 23-32	Quelle: Shelley 2002 Seite(n): 4 (internet version), Zeilen: 19-27
Members of a terrorist group are given special training on computers and software and computer engineers are hired by the groups to facilitate communications.	Members of the terrorist group are provided special training in computers and software and computer engineers are hired by the groups to facilitate communications.
International organized crime groups and terrorists both employ specialists for specific purposes. These specialists conduct intelligence operations and target surveillance, move money, or perform information technology or communications specific. The most successful of these groups have educated specialists within their ranks while others contract out for these services. Their hiring is on contractual basis, they may know accomplices or may be [hired through intermediaries, unaware of the end goals and who the end users of their services are.]	International organized crime groups and terrorists both employ specialists. These specialists conduct intelligence operations, move money, and specialize in information technology and communications. The most successful of these groups have educated specialists within their ranks while others contract out for these services. Those hired on a contractual basis may be knowing accomplices or may be hired through intermediaries, unaware who are the end users of their services.

Farbig

Anmerkungen

still copying from Shelley (2002)

[53.] Nm/Fragment 055 01

Verschleierung

Untersuchte Arbeit: Seite: 55, Zeilen: 1-7	Quelle: Shelley 2002 Seite(n): 4 (internet version), Zeilen: 25-27, 29-32
[Their hiring is on contractual basis, they may know accomplices or may be] hired through intermediaries, unaware of the end goals and who the end users of their services are.	Those hired on a contractual basis may be knowing accomplices or may be hired through intermediaries, unaware who are the end users of their services. [...]
Criminals and terrorists both engage in illicit activities. Money is the main motivation for transnational criminals; whereas for terrorists, this ordinary criminal activity is supported by their larger political and ideological objectives. Yet the crimes committed by both of the groups differ only in motive and not in substance.	Criminals and terrorists both engage in illicit activity. The transnational criminals do this solely to make money. Whereas for terrorists, this ordinary criminal activity is used to support their larger political and ideological objectives. Yet the crimes committed by these two groups differ only in motive and not in substance.

Farbig

Anmerkungen

Still continuing the copying-process. The source is not given.

[54.] Nm/Fragment 057 11

Verschleierung

Untersuchte Arbeit: Seite: 57, Zeilen: 11-29	Quelle: terrorism_research_2005 Seite(n): 1, Zeilen: 2

Farbig

The organizational structure determines the strengths and weaknesses of a group. Knowledge about prevalent models of terrorist organizations leads to a better understanding of their capabilities and targets. Knowledge of the different labels and systems of classification that have been applied to groups and individuals aid in discarding useless or irrelevant terms, and in understanding the purposes and usefulness of different terminologies.

Traditionally, a specific political agenda, ideological motivation or the desire for national or ethic liberation dominates the understanding of terrorism. Although, the discussed image is true for a number of terrorist organizations, but it is no longer universally valid. Also, a generational change in leadership of wellknown groups is in many cases ushering in a more damaging and relentless type of organization.

There are two general categories of terrorist organizations: networked and hierarchical. Newer organizations tend to employ the networked model, while strict Leninist or Maoist group tending towards hierarchical model to exercise centralized control.

The organizational structure of a group determines its strengths and weaknesses. A general knowledge of the prevalent models of terrorist organizations leads to a better understanding of their capabilities. Knowledge of the different labels and systems of classification that have been applied to groups and individuals aid us in discarding useless or irrelevant terms, and in understanding the purposes and usefulness of different terminologies.

In recent times, the popular image of a terrorist group operating according to a specific political agenda and motivated by ideology or the desire for ethnic or national liberation dominated our understanding of terrorism. While still true of some terrorist organizations, this image is no longer universally valid. Also, a generational change in leadership of established groups is in many cases ushering in a more a destructive and relentless type of organization.

There are two general categories of organization; *hierarchical* and *networked*. [...] Newer groups tend towards organizing or adapting to the possibilities inherent in the network model. [...] strict Leninist or Maoist groups tending towards centralized control and hierarchical structure.

Anmerkungen

Fairly minor changes. The source is not mentioned anywhere in the thesis.

[55.] Nm/Fragment 058 01

Verschleierung

Untersuchte Arbeit: Seite: 58, Zeilen: 1-30	Quelle: DCSINT_2005 Seite(n): 3-1, 3-2, Zeilen: p.3-1,21-31.32-36 - p.3-2,1.3-8
[Since in the case of larger structure, nearly all organizations follow the] variants of cellular organizations at strategic and tactical level to enhance security. It also facilitates better management and organization of operations. Terror groups often require political activity and hierarchical structure to coordinate violence with a political action. It may also be necessary for a politically affiliated group to observe cease-fire agreements or avoid particular targets in support of political objectives. This can be difficult to enforce in networked organizations. Terrorist groups can be at various stages of development in terms of capabilities and sophistication. Newer groups having fewer resources will usually lack capability and experience, and operate in permissive areas or under the control of more proficient organizations. Change in terrorist leadership may signal significant adjustments to organizational priorities and means of conducting terrorism. The terrorist groups associated with ethnic or nationalist agendas operating in one country or a localized region tend to require fewer capabilities as compared to larger groups. Larger groups can coalesce from smaller organizations, or smaller groups can splinter off from larger ones. **2.5 TERRORIST GROUP STRUCTURE** Members or supporters of terrorist organization can be classified into four types based on their level of commitments: passive supporters, active supporters, cadre, and leadership. Figure 2.1 shows how each successive level of commitment has fewer members. This pyramid diagram shows the relative number of people in each category and not the organizational structure. It is valid for either network or hierarchical organizational structure. Passive supporters may mix together with active supporters and are not aware of their actual relationship with the organization.	Within the larger structure, though, virtually all groups use variants of cellular organizations at the tactical level to enhance security and to organize for operations. Terrorist groups that are associated with a political activity or organization will often require a more hierarchical structure, in order to coordinate terrorist violence with political action. It also can be necessary for a politically affiliated group to observe cease-fire agreements or avoid particular targets in support of political objectives. This can be difficult to enforce in networked organizations. Terrorist groups can be at various stages of development in terms of capabilities and sophistication. Newer groups with fewer resources will usually be less capable, and operate in permissive areas or under the tutelage of more proficient organizations to develop proficiency. Change in terrorist leadership, [...] may signal significant adjustments to organizational priorities and means of conducting terrorism. Also, groups professing or associated with ethnic or nationalist agendas and limiting their operations to one country or a localized region tend to require fewer capabilities. Larger groups can coalesce from smaller organizations, or smaller groups can splinter off from larger ones. [p. 3-2] **Section I: Terrorist Group Structure** [...] There are typically different levels of commitment within an organization: passive supporters, active supporters, cadre, and leadership. Figure 3-1 shows how each successive level of commitment has fewer members. This pyramid diagram is not intended as an organizational picture, but to show the relative number of people in each category. This image of overall density holds true for networks as well as hierarchies. Passive supporters may intermingle with active supporters and be unaware of what their actual relationship is to the organization.

Farbig

Anmerkungen

The only mention of the source is in connection with the citation of figure 2.1 on the next page (page 59). The reader is left in the dark about the origin of the text.

[56.] Nm/Fragment 059 01

Verschleierung

Untersuchte Arbeit: **Seite: 59, Zeilen: 1-10**	**Quelle: DCSINT_2005** **Seite(n): 3-2, Zeilen: 23-29**	Farbig
• Passive supporters are motivated by the announced goals of the terrorist organization. They may have ideological sympathy with the terrorist organization, however they are not committed enough to take any action. Passive supporters are often unaware of their real relation with the terrorist organization. However, they are used for political activities, fund raising campaigns, gathering assisting in gathering intelligence and other nonviolent activities. Sometimes fear of reprisal from terrorists is a compelling factor in passive support.	• Passive Supporters are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization, but are not committed enough to take action. They may not be aware of their precise relation to the terrorist group, and interface with a front that hides the overt connection to the terrorist group. Sometimes fear of reprisal from terrorists is a compelling factor in passive support. Sympathizers can be useful for political activities, fund raising, and unwitting or coerced assistance in intelligence gathering or other non-violent activities.	

Anmerkungen

continuation from previous page - the source is only mentioned as reference for figure 2.1. on the same page, but not as reference for anything else.

On this and the next page, Nm will present more or less word-for-word the description of each of the four "levels of commitment", which can be found in the source, by using large chunks of the original wording and putting it together with slightly different "stuffing". Another "major" change he will introduce is the permutation of the order of the various descriptions ("bottum-up" instead of "top-down").

[57.] Nm/Fragment 059 11

Verschleierung

Untersuchte Arbeit: **Seite: 59, Zeilen: 11-18**	**Quelle: DCSINT_2005** **Seite(n): 3-2, Zeilen: 18-22**	Farbig
• Active Supporters actively participate in the political, fundraising, and information activities of the group. They may also conduct initial intelligence and surveillance activities, and provide safe houses, financial contributions, medical assistance, and transit assistance for active members of the organization. They do not commit or engage them in violence, but are usually fully aware of their relationship to the terrorist group and motives of the organization.	• Active Supporters are active in the political, fund-raising, and information activities of the group. Acting as an ally or tacit partner, they may also conduct initial intelligence and surveillance activities, and provide safehaven houses, financial contributions, medical assistance, and transit assistance for active members of the organization. They are usually fully aware of their relationship to the terrorist group but do not commit violent acts.	

Anmerkungen

continues the list of descriptions; the source is not mentioned

[58.] Nm/Fragment 060 01

Verschleierung

Untersuchte Arbeit: **Seite: 60, Zeilen: 1-4**	**Quelle: DCSINT_2005** **Seite(n): 3-2, Zeilen: 15-17**	Farbig
Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. Low-level cadres are the bombers and similar direct actors in terrorism and violent plans.	Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. Low-level cadres are the bombers and similar direct action terrorists in an attack.	

Anmerkungen

continued from the previous page; still no mention of the source.

[59.] Nm/Fragment 060 05

Verschleierung

Untersuchte Arbeit: Seite: 60, Zeilen: 5-9	Quelle: DCSINT_2005 Seite(n): 3-2, Zeilen: 9-11	Farbig
• Leaders design organizational policy and provide directions. They approve goals and objectives and provide management and guidance for operations. Usually leaders rise from within the ranks of any given organization, or create their own organization from scratch.	• Leaders provide direction and policy; approve goals and objectives; and provide overarching guidance for operations. Usually leaders rise from within the ranks of any given organization, or create their own organization from scratch.	

Anmerkungen

this finishes the list - still no mention of the source

[60.] Nm/Fragment 060 10

Verschleierung

Untersuchte Arbeit: Seite: 60, Zeilen: 10-32	Quelle: DCSINT_2005 Seite(n): 3-2, 3-3, Zeilen: p.3-2,30-37 - p.3-3,1-8	Farbig
Terrorist groups will recruit from the population having sympathy to their goals. Often legitimate organizations can serve as recruiting grounds for terrorists. For example: Militant Islamic recruiting is often associated with the proliferation of the radical Wahhabi sect. The recruitment takes place via Wahhabist schools worldwide, financed from both governmental and private donations and grants (Corpus N. Victor, 2002). In the time of need, particular skills or qualification is also considered during recruitment. Of particular concern are attempts of terrorist organizations to recruit current or former members of the armed forces, both as trained operatives, and as agents in place. Recruitment can gain operatives from many diverse social backgrounds. At times, the approach to radical behaviour or direct actions with terrorism can develop over the course of years or decades. One example is John Walker Lindh. Lindh was the U.S. citizen, captured by U.S. military forces during the war in Afghanistan. His notoriety jumped into international attention, as did the situation of individuals from several counties that were apprehended in combat actions of Afghanistan. Lindh was changed from an unassuming middle-class adolescent in the Western United States to a member of a paramilitary training camp in Pakistan and his subsequent support for Taliban forces in Afghanistan spotlights that general profiling should be tempered with specific instances [and a broad perspective.]	[p. 3-2] Terrorist groups will recruit from populations that are sympathetic to their goals. Often legitimate organizations can serve as recruiting grounds for terrorists. Militant Islamic recruiting, for example, is often associated with the proliferation of the radical Wahhabi sect. This recruiting is conducted on a worldwide basis via Wahhabist schools financed from both governmental and non-governmental donations and grants. [FN 128] Some recruiting may be conducted for particular skills and qualifications, and not be tied to ideological characteristics. Of particular concern are attempts of terrorist organizations to recruit current or former members of the U.S. armed forces, both as trained operatives, and as agents in place. [FN 128] Victor N. Corpus, “The Invisible Army” (Briefing presented at Fort Leavenworth, KS, 5 November 2002), TRADOC ADCSINT-Threats Files, Fort Leavenworth, KS. [p. 3-3] Recruitment can gain operatives from many diverse social backgrounds. At times, the approach to radical behavior or direct actions with terrorism can develop over the course of years or decades. One example is John Walker Lindh, the U.S. citizen captured by U.S. military forces in the war in Afghanistan. His notoriety jumped into international attention, as did the situation of individuals from several counties that were apprehended in combat actions of Afghanistan. Lindh’s change from an unassuming middle-class adolescent in the Western United States to a member of a paramilitary training camp in Pakistan and subsequent support for Taliban forces in Afghanistan spotlights that general profiling should be tempered with specific instances and a broad perspective.	

Anmerkungen

copying continues without any break - no mention of the source.

[61.] Nm/Fragment 061 01

Verschleierung

Untersuchte Arbeit: Seite: 61, Zeilen: 1-13	Quelle: DCSINT_2005 Seite(n): 3-3, Zeilen: 9-16	Farbig
Another stunning case was of Jose Padilla. He attempted very simple and voluntary efforts to detonate a bomb in the U.S. This illustrates Al Qaeda techniques to support, finance, and use less sophisticated means to conduct terrorist acts. Some groups will also use coercion and leverage to gain limited or one-time cooperation from useful individuals. Blackmailing and intimidation are the commonly exerted coercion forms by terrorist organizations to gain cooperation of useful individuals. This cooperation can range anywhere like acquiring the useful information to conduct a suicide bombing operation (Reich Walter, 1998). Threats to family members are also employed. Coercion is often directed at personnel in government security and intelligence organizations.	In the case of Jose Padilla, his simple and voluntary efforts to detonate a bomb in the U.S. may illustrate al Qaeda techniques to support, finance, and use less than sophisticated means to conduct terrorist acts. [FIGURE] Some groups will also use coercion and leverage to gain limited or one-time cooperation from useful individuals. This cooperation can range anywhere from gaining information to conducting a suicide bombing operation. [FN 129] Blackmail and intimidation are the most common forms of coercion. Threats to family members are also employed. Coercion is often directed at personnel in government security and intelligence organizations. [FN 129] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 270-271.	

Anmerkungen

continued from previous page - no mention of the source is made - some slight change in the order of sentences.

[62.] Nm/Fragment 061 14

Verschleierung

Untersuchte Arbeit: Seite: 61, Zeilen: 14-30	Quelle: DCSINT_2005 Seite(n): 3-4, Zeilen: 1-12, 13-14	Farbig
2.6 TACTICAL-LEVEL CELLULAR ORGANIZATION The smallest elements at the tactical level of terrorist organizations are the cells that serve as building-blocks for the terrorist organization. One of the primary reasons for a cellular or compartmentalized structure is security. The compromise or loss of one cell should not compromise the identity, location, or actions of other cells. A cellular organizational structure makes it difficult for an adversary to penetrate the entire organization. Personnel within one cell are often unaware of the existence of other cells and, therefore, cannot divulge sensitive information to infiltrators or captors. The Earth Liberation Front (ELF) is an excellent example of the cellular organization. The homepage ELF site states that ELF is modelled after Animal Liberation Front in the structured way to maximize the effectiveness. Operating in cells not only guarantees the security of group members but also such decentralized structure [helps to continue conducting actions.]	**Tactical-level Cellular Organization** The smallest elements at the tactical level of terrorist organizations are the cells that serve as building blocks for the terrorist organization. One of the primary reasons for a cellular or compartmentalized structure is security. The compromise or loss of one cell should not compromise the identity, location, or actions of other cells. A cellular organizational structure makes it difficult for an adversary to penetrate the entire organization. Personnel within one cell are often unaware of the existence of other cells and, therefore, cannot divulge sensitive information to infiltrators or captors. The home page of the Earth Liberation Front is an excellent example of this cellular organization. It states, “Modeled after the Animal Liberation Front, the E.L.F. is structured in such a way as to maximize effectiveness. By operating in cells (small groups that consist of one to several people), the security of group members is maintained. [...] This decentralized structure helps keep activists out of jail and free to continue conducting actions.”	

Anmerkungen

Minimal to no adjustments in the beginning. Later on Nm diverges from the original - but only a little bit. The source is not mentioned at all. The passage continues on the next page.

[63.] Nm/Fragment 062 01

Verschleierung

Untersuchte Arbeit: Seite: 62, Zeilen: 1-16	Quelle: DCSINT_2005 Seite(n): 3-4, Zeilen: 13-25	Farbig
[Operating in cells not only guarantees the security of group members but also such decentralized structure] helps to continue conducting actions.	This decentralized structure helps keep activists out of jail and free to continue conducting actions."	
Terrorists may organize cells based on family or employment relationships, on a geographic basis, or by specific functions such as direct action and intelligence. Terrorist groups may also form multifunctional cells and these cells may be used by terrorist groups to control its members. Cell members remain in close contact with each other in order to provide emotional support and to prevent desertion or breach of security procedures. Cell leaders are normally the people who communicate and coordinate with higher levels and other cells.	Terrorists may organize cells based on family or employment relationships, on a geographic basis, or by specific functions such as direct action and intelligence. The terrorist group may also form multifunctional cells. The terrorist group uses the cells to control its members. Cell members remain in close contact with each other in order to provide emotional support and to prevent desertion or breach of security procedures. The cell leader is normally the only person who communicates and coordinates with higher levels and other cells.	
A terrorist group may form only one cell or may form many cells that operate locally, trans-nationally, or internationally. The composition, size and number of cells in the terrorist organization depend on the size of the terrorist group itself. An international terrorist group operating in more than within one country has more cells than the one operating in a single country or limited territory.	A terrorist group may form only one cell or may form many cells that operate locally, transnationally, or internationally. The number of cells and their composition depend on the size of the terrorist group. A terrorist group operating within one country frequently has fewer cells and specialized teams than does an international terrorist group that may operate in several countries.	

Anmerkungen

Minimal adjustments. The source is not mentioned. The portion taken from the source starts in the middle of a quotation from the home page of the Earth Liberation Front

[64.] Nm/Fragment 062 17

Verschleierung

Untersuchte Arbeit: Seite: 62, Zeilen: 17-29	Quelle: DCSINT_2005 Seite(n): 3-4, Zeilen: 26-35	Farbig
2.7 GROUP ORGANIZATIONAL STRUCTURE	**Group Organizational Structure**	
As stated earlier, there are two basic models used when examining the overall organizational structure of a terrorist group. These are the hierarchical and the networked models. A terrorist group may employ either type or a combination of the two models.	As stated earlier, there are two basic models used when examining the overall organizational structure of a terrorist group. These are the hierarchical and the networked models. A terrorist group may employ either type or a combination of the two models.	
2.7.1 Hierarchical Structure	*Hierarchical Structure*	
Hierarchical structure organizations maintain a well-defined vertical chain of command, authority and responsibility. Data and intelligence flows up and down organizational channels that correspond to these non-horizontal chains, but may not move horizontally through the organization. This is more traditional, and is common of groups that are well established with a command and support structure.	Hierarchical structure organizations are those that have a well-defined vertical chain of command linkage and responsibility. Data and intelligence flows up and down organizational channels that correspond to these vertical chains, but may not move horizontally through the organization. This is more traditional, and is common of groups that are well established with a command and support structure.	

Anmerkungen

text nearly identical, but the source is not mentioned.

[65.] Nm/Fragment 063 01

Verschleierung

Untersuchte Arbeit: Seite: 63, Zeilen: 1-29	Quelle: DCSINT_2005 Seite(n): 3-4, 3-5, Zeilen: 3-4: 36-39, 3-5: 1-19
Hierarchical structure offers the organizations greater specialization of functions in their subordinate cells (support, operations, intelligence). Usually, the leader of cell is aware of other cells or contacts of the organization (may be to a limited extent) and only senior leadership has visibility of the organization at large. In the past, terrorism was practiced in this manner by identifiable organizations with a command and control structure influenced by ideology or theory of revolution. Radical leftist organizations such as the Japanese Red Army, the Red Army Faction in Germany, the Red Brigades in Italy, as well as ethno-nationalist terrorist movements such as the Palestine Liberation Organization, the Irish Republican Army and the Basque separatist ETA group, conformed to this stereotype of the "traditional" terrorist group. These organizations had a clearly defined set of political, social or economic objectives, and tailored aspects of their organizations (such as a “political” wing or “social welfare” group) to facilitate their success. The necessity to coordinate actions between various “fronts,” some of which were political and allegedly non-violent, and the use of violence by terrorists and some insurgents, favoured a hierarchical command structure.	Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence). Usually, only the cell leader has knowledge of other cells or contacts, and only senior leadership has visibility of the organization at large. In the past, terrorism was practiced in this manner by identifiable organizations with a command and
2.7.2 Networked Structure	[Page 3-5]
Terrorists are in this decade become increasingly part of far more joint and wider system of networks than experienced before. Groups based on religious or single-issue motives lack a specific political or patriotic agenda; non-horizontal structure is thus less needed. Instead, they can depend and even thrive on loose association with like-minded clusters or people from a diversity of places. General objectives and goals are announced, and operation and initiative is left to the individuals or cells.	control structure influenced by revolutionary theory or ideology. Radical leftist organizations such as the Japanese Red Army, the Red Army Faction in Germany, the Red Brigades in Italy, as well as ethno-nationalist terrorist movements such as the Palestine Liberation Organization, the Irish Republican Army and the Basque separatist ETA group, conformed to this stereotype of the "traditional" terrorist group. These organizations had a clearly defined set of political, social or economic objectives, and tailored aspects of their organizations (such as a “political” wing or “social welfare” group) to facilitate their success. The necessity to coordinate actions between various “fronts,” some of which were political and allegedly nonviolent, and the use of violence by terrorists and some insurgents, favored a strong and hierarchical authority structure.
	Networked Structure
	Terrorists are now increasingly part of far more indistinct and broader system of networks than previously experienced. Groups based on religious or single-issue motives lack a specific political or nationalistic agenda; they therefore have less need for a hierarchical structure to coordinate the achievement of their goals. Instead, they can depend and even thrive on loose affiliation with like-minded groups or individuals from a variety of locations. General goals and targets are announced, and individuals or cells are expected to use flexibility and initiative to conduct the necessary action.

Farbig

Anmerkungen

The source is not mentioned.

[66.] Nm/Fragment 064 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 64, Zeilen: 1	Quelle: DCSINT_2005 Seite(n): 3-5, Zeilen: -
[FIGURE, identical to source]	[FIGURE]
Figure 2.2. Typical Categories of Terrorist Organization	Figure 3-2. Typical Categories of Terrorist Organization

Farbig

Anmerkungen

The figure in the thesis has been taken via copy-paste from the source, except for the last pixel line, which was part of the frame. The source is not given.

[67.] Nm/Fragment 064 02

Verschleierung

Untersuchte Arbeit: **Seite: 64, Zeilen: 2-16**	**Quelle: Arquilla_Ronfeldt_2001** **Seite(n): 69, Zeilen: 1ff**
2.8 DIMENSIONS OF CRIMINAL/ TERRORIST NETWORKS	Dimensions of Criminal Networks
Although networks are an important, and somewhat neglected, form of criminal organization, they are not the single or exclusive system. The traditional non-horizontal model long associated with Mafia families in the U.S., for example, does not need to be abandoned: After all, it is possible to have networks of hierarchies, hybrid organizational forms with some hierarchical mechanisms and a substantial network aspect, and even a network of networks. The shapes and sizes of the networks can be diverse; however, they vary along several critical scopes.	Although networks are an important, and somewhat neglected, form of criminal organization, they are not the sole or exclusive form. The traditional hierarchical model long associated with Mafia families in the United States, for example, does not need to be jettisoned: After all, it is possible to have networks of hierarchies, hybrid organizational forms with some hierarchical components and a significant network dimension, and even a network of networks. If networks come in a great variety of shapes, however, they vary along several critical dimensions.
First, a network can be created and directed by a core of coordinators/ organizers who want to use it for specific purposes (a “directed network”) or it can emerge spontaneously as a mechanism to add efficiency to the functioning of a market (a [“business network”).]	First, a network can be created and directed by a core of organizers who want to use it for specific purposes (a “directed network”) or it can emerge spontaneously as a mechanism to add efficiency to the functioning of a market (a “transaction network”).

Anmerkungen

Slight adaptations. The source is not given.

[68.] Nm/Fragment 065 01

Verschleierung

Untersuchte Arbeit: **Seite: 65, Zeilen: 1-33**	**Quelle: Arquilla_Ronfeldt_2001** **Seite(n): 69, 70, Zeilen: 14ff; 1ff**

Farbig

The Colombian cocaine trade can be seen as an example of directed network. Its core members at least came into being to carrying of cocaine to U.S. in the 1980s and early 1990s and directed the whole network to achieve the objective. Whereas, the heroin trade from Southeast Asia, in contrast, is far more of a business network, in which agents (we may call them brokers) play a critical role at almost every stage of the process. Herion [sic!] reaches the retail market by passing through a sequence of brokers/ agents and independent suppliers are responsible for moving it from manufacturers to agents. In practice, a directed network can be part of a larger business network, and it seems that with the demise of the large, vertically cohesive networks functioning out of Medellín and Cali, the Colombian cocaine trade has increasingly taken on this hybrid value.

Second, networks can range from small, inadequate relations at the local level to transnational provider networks responsible for moving both legal and illegal belongings across national borders. Membership can be determined by a particular characteristic, such as ethnicity, or can be relatively open. The networks are likely to be multi-ethnic when influential considerations balance the need to maintain a high degree of selectiveness.

Among the larger criminal networks, it is possible to identify both key individuals and key corporations or firms through which they operate. One of the best examples of a widespread transnational criminal network is that revolving around Semeon Mogilevich. Based in Hungary, Mogilevich is reputed to have close links with the Solntsevo criminal organization in Moscow, with prostitution activities in Frankfurt, with the Genovese family in New York, and with Russian criminals in Israel. For several years, Mogilevich operated in part through a company called Magnex YBM operating in the United States and Canada. The company was engaged in money laundering and stock frauds. It also had a network of companies in the Bahamas, the British Channel Islands, and the [Caymans.]

The Colombian cocaine trade in the 1980s and early 1990s was very much a directed network—at least at the core—which came into existence to transport cocaine to the United States. The heroin trade from Southeast Asia, in contrast, is far more of a transaction network, in which brokers play a critical role at almost every stage of the process. Producers supply heroin to independent distributors, and it is then passed along a chain of brokers until it reaches the retail market. In practice, of course, a directed network can be part of a larger transaction network, and it appears that with the demise of the large, vertically integrated networks operating out of Medellin and Cali, the Colombian cocaine trade has increasingly taken on this hybrid quality.

Second, networks can range from small, very limited associations at the local level to transnational supplier networks that move a variety of goods, either licit or illicit—or even both—across national borders. Membership can be determined by a particular characteristic, such as ethnicity, or can be relatively open. Supplier networks are likely to be multiethnic when instrumental considerations outweigh the desire or need to maintain a high degree of exclusiveness.

Among the larger criminal networks, it is possible to identify both key individuals and key companies or firms through which they operate. One of the best examples of an extensive transnational criminal network is that revolving around Semeon Mogilevich. Based in Hungary,

[Page 70]

Mogilevich is reputed to have close links with the Solntsevo criminal organization in Moscow, with prostitution activities in Frankfurt, with the Genovese family in New York, and with Russian criminals in Israel. For several years, Mogilevich operated in part through a company called Magnex YBM operating in the United States and Canada (where it was engaged in money laundering [...] and stock fraud) and also had a network of companies in the Bahamas, the British Channel Islands, and the Caymans.

Anmerkungen

Slight adaptations. The source is not referenced.

[69.] Nm/Fragment 066 01

Verschleierung

Untersuchte Arbeit: Seite: 66, Zeilen: 1-33	Quelle: Arquilla_Ronfeldt_2001 Seite(n): 70, 71, Zeilen: 9ff, 1-2
In such situation, Mogilevich was far less vulnerable than the leader of traditional Mafia group, in spite of its important role in such transnational network. Despite of continued claims about his role, he has never been sentenced of any corruption/ crime.	Significantly, as a key figure in this transnational network, Mogilevich is far less vulnerable than a traditional Mafia don or family head, and, despite continued allegations about his role, he has never been convicted of any crime.
Third, networks can be highly structured and enduring in nature orthey can be loose, fluid, or imprecise in character, with members coming and going according to particular requirements, prospects, and/ or demands. Some individuals or even small organizations will point in and out of networks when it is convenient for them to do so. Other networks will have a more enduring membership. In yet other cases, there will be some members who provide continuity and direction to the network, while others will play an irregular or transitory part. There will be both “embedded ties” and continuing relations based on high levels of trust, mutual respect, and mutual concern; but also more transitory connections based on nothing more than a short-term chance of interests. An analogous dynamism is obvious in the way in which criminals develop businesses to make maximum of prospects and closing them whenever is needed or when they are directed in those particular areas.	Third, networks can be highly structured and enduring in nature or they can be loose, fluid, or amorphous in character, with members coming and going according to particular needs, opportunities, and demands. Some individuals or even small organizations will drift in and out of networks when it is convenient for them to do so. Other networks will have a more enduring membership. In yet other cases, there will be some members who provide continuity (and direction) to the network, while others will play an occasional or ephemeral part. There will be both “embedded ties” and enduring relations based on high levels of trust, mutual respect, and mutual concern; but also more fleeting relations based on nothing more than a shortterm coincidence of interests. A similar dynamism is evident in the way in which criminals develop and use front companies, creating them wherever opportunities exist and abandoning or closing them whenever they become the targets of law enforcement investigations.
Last, networks can be motivated barely on a sole purpose or on the supply of a particular product, or they can supply a broader range of illegitimate goods or engage in more diverse criminal activities. For example Colombian and Mexican drug trafficking organizations do not engage themselves into a wide range of activities. Although there has been a tendency to traffic in more than one kind of drug, essentially they are in the drug trafficking business and little else. On the other hand Russian and Chinese criminal organizations are involved in very diverse criminal activities like drug trafficking, dealing in lifted/ stolen cars and weapons, prostitution, antiquities, and vanishing classes, yet also engaging in numerous systems of extortion and even in monetary [fraud.]	Last, networks can be focused very narrowly on a single purpose or on the supply of a single product, or they can supply a broader range of illegal products or engage in more diverse criminal activities. Colombian and Mexican drug trafficking organizations, for example, engage in a very narrow range of activities. Although there has been a tendency to traffic in more than one kind of drug, essentially they are in the drug trafficking business and little else. Russian and Chinese criminal organizations, in contrast, have a very diverse portfolio of criminal activities, trafficking in drugs, stolen cars, arms, prostitution, antiqui- [Page 71] ties, and endangered species, yet also engaging in various forms of extortion and financial fraud.

Anmerkungen

Somewhat adjusted. Source is not referenced.

[70.] Nm/Fragment 067 02

Verschleierung

Untersuchte Arbeit:
Seite: 67, Zeilen: 2-32

Networks with their particular characteristics offer substantial eyecatching choices to terrorists. For example, range, flexibility, low visibility, durability, etc. are well known some of the attractive characteristics.

Networks can often operate clandestinely. The more visible a criminal enterprise the more likely it is to be attacked by law enforcement. It is well known fact that “Networks are not immediately visible”, which is considered strongly by criminal enterprises and can be used to hide behind various licit activities. Those can operate with a lower degree of formality than other types of organization, and can maintain a profile that does not bring them to the attention of law enforcement. In some cases, of course, the network will be exposed. However, in the beginning of the investigation of Mogilevich network by FBI, there was considerable surprise at its extensiveness.

Even when they are targeted by law enforcement, many criminal networks are inherently dispersed, with the result that they do not provide obvious centres of gravity or loci for law enforcement attacks. Lacking a physical substructure or a large investment of sunk costs that would add significantly to their weakness, networks can also migrate easily from zones where risks from law enforcement are maximum to zones where the risks are much lesser.

Criminal networks, especially when they are transnational in character, can exploit differences in national laws and regulations. For example Russian criminals travelled to Israel during 1990’s, which was lacking in money laundering laws and measures. Israel criminalized money laundering in 2000. In some cases, money from Russia was used in Israel to buy up virtually bankrupt businesses that would then start to make “profits” that flowed back to Russia. In some instances transnational criminal organizations also create jurisdictional confusion, making it difficult for any [single nation’s law enforcement agencies to act effectively against them.]

Quelle: Arquilla_Ronfeldt_2001
Seite(n): 71, Zeilen: 3ff

Farbig

Whatever their precise characteristics, networks provide criminals with diversity, flexibility, low visibility, durability, and the like. Indeed, their attractions are very considerable:

- Networks can often operate clandestinely. The more visible a criminal enterprise the more likely it is to be attacked by law enforcement. One of the most significant points about networks, however, is that they are not immediately and obviously visible. Criminal networks can hide behind various licit activities, can operate with a lower degree of formality than other types of organization, and can maintain a profile that does not bring them to the attention of law enforcement. In some cases, of course, the network will be exposed. Significantly, though, when the FBI began to investigate the Mogilevich criminal network, there was considerable surprise at its extensiveness.
- Even when they are targeted by law enforcement, many criminal networks are inherently dispersed, with the result that they do not provide obvious centers of gravity or loci for law enforcement attacks. Lacking a physical infrastructure or a large investment of sunk costs that would add significantly to their vulnerability, networks can also migrate easily from areas where risks from law enforcement are high to areas where the risks are much lower.
- Criminal networks, especially when they are transnational in character, can exploit differences in national laws and regulations (Israel, for example, only criminalized money laundering in 2000) by engaging in what might be termed jurisdictional arbitrage. Throughout the 1990s, for example, criminals from the former Soviet Union flooded into Israel, exploiting both the law of return and the lack of anti-money laundering measures. In some cases, money from Russia was used in Israel to buy up virtually bankrupt businesses that would then start to make “profits” that flowed back to Russia. In some instances transnational criminal organizations also create jurisdictional confusion, making it difficult for any single nation’s law enforcement agencies to act effectively against them.

Anmerkungen

Somewhat adjusted. Source is not referenced.

In the first sentence "criminals" is replaced by "terrorist" and like that the focus of the section is adapted to what is needed for the thesis. In the third paragraph the American spelling ("center") is anglicized.

[71.] Nm/Fragment 068 01

Verschleierung

Untersuchte Arbeit: Seite: 68, Zeilen: 1-17	Quelle: Arquilla_Ronfeldt_2001 Seite(n): 71-72, Zeilen: 33ff;
[In some instances transnational criminal organizations also create jurisdictional confusion, making it difficult for any] single nation's law enforcement agencies to act effectively against them. Laundering money through a series of firms and banks in multiple jurisdictions, for example, makes it arduous and costly for law enforcement to follow up the money trail. Networks also offer opportunities for both redundancy and flexibility. In network structures, it is easier to create redundancies than it is in more formal and rigid organizations. It can operate, even when a part of same network is destroyed, at the same time it can become very resilient and can be easily rebuilt. In view of these benefits, it is not unexpected that network structures have become particularly predominant in modern organized crime, whether in the United States, Europe, or states in transition such as Russia, Ukraine, other newly independent states of the former Soviet Union, South Africa, and Cambodia, or even China and Cuba. As reported in the referenced book, the analysis now looks at the main characteristics of criminal networks; characteristics that help make them extremely difficult to combat.	In some instances transnational criminal organizations also create jurisdictional confusion, making it difficult for any single nation's law enforcement agencies to act effectively against them. Laundering money through a series of firms and banks in multiple jurisdictions, for example, makes it arduous and costly for law enforcement to follow the money trail. [Seite 72] ▪ Networks also offer opportunities for both redundancy and resilience. In network structures, it is easier to create redundancies than it is in more formal and rigid organizations — so that even if part of the network is destroyed it can still operate. Furthermore, degradation of a network does not necessarily lead to its demise: Networks are very resilient and can easily be rebuilt. In view of these advantages, it is not surprising that network structures have become particularly prevalent in contemporary organized crime, whether in the United States, Europe, or states in transition such as Russia, Ukraine, other newly independent states of the former Soviet Union, South Africa, and Cambodia, or even China and Cuba. Accordingly, the analysis now looks at the main characteristics of criminal networks, characteristics that help make them extremely difficult to combat.

Farbig

Anmerkungen

Some adjustments. The source has not been referenced

[72.] Nm/Fragment 068 18

Verschleierung

Untersuchte Arbeit: Seite: 68, Zeilen: 18-30	Quelle: DCSINT_2005 Seite(n): 2-12, Zeilen: 18-27
2.9 TERRORIST CHARACTERISTICS Terrorists do not have a single or general personality profile. Meaning, no single analytical test exist which promises empathy of a terrorist. Although, many terrorism related studies have been conducted by analyzing the biographical and social data on known terrorists, with goal to develop some form of terrorist profile. However, none of them truly succeeded as they have just shown that in general, terrorists are people who often feel isolated from society and have a complaint or regard themselves as victims of an inequality. Political or religious reasons help as a commitment to the terrorists and they do not regard their violent actions as criminal. They show no pity or regret for their actions. Although their level of [complexity will vary depending on the individual and the specific terrorist group, terrorists are people who are skilled and brutal in leading terrorist acts (Hudson, A. R, 1999).]	**Section III: Terrorist Characteristics** No singular personality profile of a terrorist exists, and no predictive test exists that can guarantee identification of a terrorist. Numerous terrorism-related studies have analyzed the biographical and social data on known terrorists in an attempt to develop some form of terrorist profile. Studies have shown that in general, terrorists are people who often feel alienated from society and have a grievance or regard themselves as victims of an injustice. They are devoted to their political or religious cause and do not regard their violent actions as criminal, showing no pity or remorse for their actions. Although their level of sophistication will vary depending on the individual and the specific terrorist group, terrorists are people who are skillful and ruthless in conducting terrorist acts.[FN 115] [FN 115] Rex A. Hudson, *The Sociology and Pshychology[sic] of Terrorism: Who Becomes a Terrorist and Why?* (Washington: Library of Congress Federal Research Division, 1999), 50.

Farbig

Anmerkungen

With the source never mentioned, the whole of section III of the source is to be found - mostly word-for-word - in the thesis under scrutiny. This is the starting-point. The source misspells a word in Hudson's book, Nm corrects this word in the bibliography but does not give the year.

[73.] Nm/Fragment 069 01

Verschleierung

Untersuchte Arbeit: Seite: 69, Zeilen: 1-6	Quelle: DCSINT_2005 Seite(n): 2-12, Zeilen: 25-29
[Although their level of] complexity will vary depending on the individual and the specific terrorist group, terrorists are people who are skilled and brutal in leading terrorist acts (Hudson, A. R, 1999). In addition to the above qualities, there are some general characteristics that are equally common among terrorists. There are also some common stereotypes and misconceptions regarding terrorists.	Although their level of sophistication will vary depending on the individual and the specific terrorist group, terrorists are people who are skillful and ruthless in conducting terrorist acts. [FN 115] In addition to the above traits, there are some general characteristics that are fairly common among terrorists. There are also some common stereotypes and misperceptions regarding terrorists. [FN 115] Rex A. Hudson, *The Sociology and Pshychology of Terrorism: Who Becomes a Terrorist and Why?* (Washington: Library of Congress Federal Research Division, 1999), 50.

Farbig

Anmerkungen

continuation from previous page; the source is not mentioned

[74.] Nm/Fragment 069 06

Verschleierung

Untersuchte Arbeit: Seite: 69, Zeilen: 6-11	Quelle: Lemieux_2003 Seite(n): 5, Zeilen: 16-19
Some authors, particularly Sparrow (1991), Coles (2001), Klerks (2001) and Williams (2001) have identified a certain number of characteristics of criminal networks but these characteristics are either very general, for social networks, or much more specific for criminal networks. The main characteristics are presented below:	Some authors, particularly Sparrow (1991), Coles (2001), Klerks (2001) and Williams (2001), have identified a certain number of characteristics of criminal networks and have demonstrated how they can be analyzed. These characteristics are either very general, for social networks, or much more specific for criminal networks. We will present the main characteristics, [...]

Farbig

Anmerkungen

Some adjustments, but all content including four literature references can also be found in the source, which is not referenced.

[75.] Nm/Fragment 069 12

Verschleierung

Untersuchte Arbeit: **Seite: 69, Zeilen: 12-30**	**Quelle: DCSINT_2005** **Seite(n): 2-12, 2-13, Zeilen: p.2-12,30-39 - p.2-13,1-8**
2.9.1 Status Terrorists belong to middle or extremely wealthy background; opposite to common understanding that terrorist are sufferers of poverty and despair. While guerrilla fighters and gang members often come from poor and disadvantaged backgrounds, and may adopt terrorism as a tactic. According to the study conducted by Marc Sageman, a Senior Fellow at PFRI and a former CIA case officer in Afghanistan, out of 400 Islamic terrorists 75% came from the upper or middle class and 90% came from caring, intact families (Sagman, M, 2004). The less educated and socially dispossessed people may be used to conduct acts of terrorism. Even in terrorist groups that espouse the virtues of “the people” or “the proletariat,” leadership consists primarily of those of middle class backgrounds. However, this characteristic must be considered in context with the originating society “Middle class” and “privilege” are relative term. Both mean completely different levels of income between Western Africa and Western Europe.	[p. 2-12] **Status** Contrary to the oft-repeated charge that terrorism is a product of poverty and despair, terrorists are most commonly from middle class backgrounds, with some actually coming from extreme wealth and privilege. While guerilla fighters and gang members often come from poor and disadvantaged backgrounds, and may adopt terrorism as a tactic, terrorist groups that specifically organize as such generally come from middle and upper social and economic strata. Marc Sageman, a Senior Fellow at PFRI and a former CIA case officer in Afghanistan, conducted a study of 400 Islamic terrorists. He found that 75% came from the upper or middle class and 90% came from caring, intact families. [FN 116] The leadership may use less educated and socially dispossessed people to conduct acts of terrorism. Even in terrorist
2.9.2 Education and Intellect Generaly Terrorists are educated to more than average level, except [very few Western terrorists, which are uneducated or illiterate (Hudson, A. R, 1999).]	[FN 116] Marc Sageman, “Understanding Terror Networks,” 3. [p. 2-13] groups that espouse the virtues of “the people” or “the proletariat,” leadership consists primarily of those of middle class backgrounds. However, this characteristic must be considered in context with the society the terrorist originates from. “Middle class” or “privilege” are relative terms and will, for example, mean completely different levels of income between Western Africa and Western Europe. **Education and Intellect** Terrorists in general have more than average education, and very few Western terrorists are uneducated or illiterate.[FN 117] [FN 117] Rex A. Hudson, *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?*, 48.
Anmerkungen continuation of fragment above; source is not mentioned in this context	

[76.] Nm/Fragment 070 01

Verschleierung

Untersuchte Arbeit: Seite: 70, Zeilen: 1-32	Quelle: DCSINT_2005 Seite(n): 2-13, Zeilen: 7-31
[Generaly Terrorists are educated to more than average level, except] very few Western terrorists, which are uneducated or illiterate (Hudson, A. R, 1999). Some core members of larger terrorist organizations may have minimal education, but this characteristic is not the standard. Left wing terrorists, international terrorists, and the leadership echelon of right wing groups are usually of average or better intelligence, and have been exposed to advanced education. In fact, terrorist groups are increasingly recruiting members with expertise in areas such as communications, computer programming, engineering, finance, and the sciences (Hudson, A. R, 1999). The study of Sageman revealed 63% of his group had gone to college and 75% of those were professionals or semi-professionals (Sagman, M, 2004): For example, Osama Bin Laden is a civil engineer; Ayman Zawahiri is a physician. These terrorists generally have had exposure to higher learning, although they are usually not highly intellectual, and are frequently dropouts or possess poor academic records. Again, this is subject to the norms of the society they originate from. In societies where religious fundamentalism is prevalent, the higher education may have been advanced religious training (Harmon, C. Christopher, 2001).	Terrorists in general have more than average education, and very few Western terrorists are uneducated or illiterate. [FN 117] Some leaders of larger terrorist organizations may have minimal education, but this characteristic is not the norm. Left wing terrorists, international terrorists, and the leadership echelon of right wing groups are usually of average or better intelligence, and have been exposed to advanced education. In fact, terrorist groups are increasingly recruiting members with expertise in areas such as communications, computer programming, engineering, finance, and the sciences. [FN 118] The Sageman analysis reflected 63% of his group had gone to college and three-quarters were professionals or semi-professionals. [FN 119] (Usama bin laden a civil engineer; Ayman Zawahiri a physician; and Yasir Arafat was at one time a civil engineer.) These terrorists generally have had exposure to higher learning, although they are usually not highly intellectual, and are frequently dropouts or possess poor academic records. Again, this is subject to the norms of the society they originate from. In societies where religious fundamentalism is prevalent, the higher education may have been advanced religious training. [FN 120]
Domestic and right wing terrorists in general belong to lower educational and social levels, although they are not completely uneducated. The right wing domestic groups in the U.S. first explored the organizational and communication potential of the Internet. They will typically have received a high school level education. They were also well versed and indoctrinated in the ideological arguments they support.	Domestic and right wing terrorists tend to come from lower educational and social levels, although they are not uneducated. It was right wing domestic groups in the U.S. that first explored the communication and organizational potential of the Internet. They will typically have received a high school level education, and be very well indoctrinated in the ideological arguments they support.
2.9.3 Age	**Age**
Terrorists tend to be young. The terrorists which take part in operations are found to be within age group of 20-35, while the leaders, supporters or training cadres range from 40-50 years old. (Lacquer Walter, 1999). The amount of practical experience and [training that contributes to making an effective operative is not usually present in individuals younger than the early 20s.]	Terrorists tend to be young. Leadership, support, and training cadres can range into the 40-50 year old age groups, but most operational members of terrorist organizations are in the 20-35 year old age group.[FN 121] The amount of practical experience and training that contributes to making an effective operative is not usually present in individuals younger than the early 20s. [FN 117] Rex A. Hudson, *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?*, 48. [FN 118] Ibid., 4. [FN 119] Marc Sageman, “Understanding Terror Networks,” 3. [FN 120] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 208. [FN 121] Walter Lacquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 1999), 38.

Anmerkungen

continuation from previous page - the source is not mentioned. Whole paragraphs are taken word-for-word.

[77.] Nm/Fragment 071 01

Verschleierung

Untersuchte Arbeit: Seite: 71, Zeilen: 1-16	Quelle: DCSINT_2005 Seite(n): 2-13, 2-14, Zeilen: p.2-13,29-35 - p.2-14,1-4	Farbig
[The amount of practical experience and] training that contributes to making an effective operative is not usually present in individuals younger than the early 20s. Individuals in their teen-age have been employed as soldiers in guerrilla groups, but terrorist organizations usually do not tend to accept extremely young members, although they will use them as non-operational supporters or suicide bombers. Groups that utilize suicide operations will employ very young individuals as suicide assets, but these youths are not actually members of the organization, but are simply exploited or coerced into an operational role (Reich Walter, 1998). Many countries in the developing world subjected to ethnic, political, and religious violence; however, are seeing younger members being recruited by terrorist organizations. Pre-teens and adolescents are often receptive to terrorist recruiting because they have witnessed killings and see violence as the only way to deal with grievances (Hudson, A. R, 1999).	[p. 2-13] The amount of practical experience and training that contributes to making an effective operative is not usually present in individuals younger than the early 20s. Individuals in their teens have been employed as soldiers in guerilla groups, but terrorist organizations do not tend to accept extremely young members, although they will use them as non-operational supporters. Groups that utilize suicide operations will employ very young individuals as suicide assets, but these youths are not actually members of the organization, but simply exploited or coerced into an operational role. [FN 122] Many countries in the developing [FN 122] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 270. [p. 2-14] world subjected to ethnic, political, and religious violence; however, are seeing younger members being recruited by terrorist organizations. Pre-teens and adolescents are often receptive to terrorist recruiting because they have witnessed killings and see violence as the only way to deal with grievances. [FN 123] [FN 123] Rex A. Hudson, *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?*, 48.	

Anmerkungen

continued from previous page - the source is not mentioned.

[78.] Nm/Fragment 071 17

Verschleierung

Untersuchte Arbeit: Seite: 71, Zeilen: 17-32	Quelle: DCSINT_2005 Seite(n): 2-14, Zeilen: 8-20	Farbig
2.9.4 Gender Terrorists are not exclusively male. Usually Women's roles will often be constrained to support or intelligence and surveillance work, but some fundamentalist Islamic groups use women in operational roles. In groups where religious constraints do not affect women's roles, female membership may be above 50%, with women fully integrated into operations. Female leadership of terrorist groups is not uncommon and female terrorists do not lay behind male counterparts in terms of violence and ruthlessness. For example, one-third of the Liberation Tiger of Tamil Eelam (LTTE) cadre is made up of women and it is reported that nearly 4,000 have been killed since they began taking part in combat in 1985, over 100 of those killed belonging to the dreaded Black Tiger suicide squad (http://www.eelam.com /ltte). In August 2004, female Chechen suicide bombers were responsible for detonating improvised explosive devices (IEDs) while on [Russian commercial flights that resulted in two aircraft crashes and the death of all people on board.]	**Gender** Terrorists are not exclusively male, even in groups that are rigorously Islamic. Women's roles in these groups will often be constrained to support or intelligence work, but some fundamentalist Islamic groups use women in operational roles. In groups where religious constraints do not affect women's roles, female membership may be above fifty percent, with women fully integrated into operations. Female leadership of terrorist groups is not uncommon, and female terrorists lack for nothing in terms of violence and ruthlessness. For example, one-third of the LTTE cadre is made up of women and it is reported that nearly 4,000 have been killed since they began taking part in combat in 1985, over 100 of those killed belonging to the dreaded Black Tiger suicide squad. [FN 125] In August 2004, female Chechen suicide bombers were responsible for detonating IEDs while on Russian commercial flights that resulted in two aircraft crashes and the death of all people on board. [FN 124] 124 "Liberation Tigers of Tamil Eelam (LTTE)," South Asia Terrorism Portal, n.d., 2; available from http://www.satp.org/satporgtp/ countries/shrilanka/ terroristoutfits/Ltte.htm; Internet; accessed 7 July 2004. [FN 125] Ibid., 2.	

Anmerkungen

Only minimal changes

[79.] Nm/Fragment 072 01

Verschleierung

Untersuchte Arbeit: Seite: 72, Zeilen: 1-26	Quelle: DCSINT_2005 Seite(n): 2-14, 2-15, Zeilen: p.2-14,18-35 - p.2-15,1-3

[In August 2004, female Chechen suicide bombers were responsible for detonating improvised explosive devices (IEDs) while on] Russian commercial flights that resulted in two aircraft crashes and the death of all people on board. Within one week, another female Chechen suicide bomber detonated an IED near a metro station in northeast Moscow causing extensive property damage and injuring many people in the area (Alfano, B., 2004). However, female participation and leadership is less common in some right wing groups, particularly those with neo-Nazi and Christian Identity oriented ideologies.

2.9.5 Appearance

Terrorist usually do not appear out of the ordinary, and are capable of normal social behaviour and appearance. Thus, terrorists are often unremarkable in individual characteristics. Racial diversity in organizations such as Al Qaeda signal that attempts to racially profile likely terrorist group members is not an effective indicator. Over the long term, elements of fanatical behaviour or ruthlessness may become evident, but they are typically not immediately obvious to casual observation. An excellent example of this is the group 17 November in Greece. When the police captured 14 suspected members in 2002, the most striking characteristic was their ordinary nature. Among the group there was a school teacher, a shopkeeper, a telephone operator, and other members that appeared to be members of mainstream society. Most terrorists do not marry, even though there have been some examples of married couples within terrorist organizations. Although members of sleeper cells or other hidden operators may marry as part of their persona,

[p. 2-14]

In August 2004, female Chechen suicide bombers were responsible for detonating IEDs while on Russian commercial flights that resulted in two aircraft crashes and the death of all people on board. Within one week, another female Chechen suicide bomber detonated an IED near metro station in northeast Moscow causing extensive property damage and injuring many people in the area. [FN 126]

Again, there is an exception to this general observation in some right wing groups, particularly those with neo-Nazi and Christian Identity oriented ideologies. Female participation and leadership is much less common in these groups.

Appearance

Terrorists are often unremarkable in individual characteristics. Racial diversity in organizations such as al Qaeda signal that attempts to racially profile likely terrorist group members is not an effective indicator. They usually do not appear out of the ordinary, and are capable of normal social behavior and appearance. Over the long term, elements of fanatical behavior or ruthlessness may become evident, but they are typically not immediately obvious to casual observation. An excellent example of this is the group 17 November in Greece. When the police captured 14 suspected members in 2002, the most striking characteristic was their ordinary nature. Among the group were a schoolteacher, a shopkeeper, a telephone operator, and other members that appeared to be members of

[FN 126] Billy Alfano, Briefing: “Terrorism Strikes Russia, Summary of the Attacks from August 24 to September 3, 2004,” Department of state, Diplomatic Security, Overseas Security Advisory Council, International Security Specialist for Western Europe, n.d.

[p. 2-15]

mainstream society. [FN 127] Although members of sleeper cells or other covert operators may marry as part of their persona, most terrorists do not marry, even though there have been cases of married couples within terrorist organizations.

[FN 127] “Revolutionary Organization 17 November (17N),” CDI Terrorism Project, 5 August 2002; available from http://www.cdi.org /terrorism/17N-pr.cfm; Internet; accessed 24 September 2004.

Anmerkungen

continuation from previous page; Nm not only copies word-for-word, but follows exactly the line of argumentation found in the source - thus a passage on "Appearance" follows a passage on "Gender". The last sentence in the sub-chapter ends with a comma that is also found in the source, but the second half of the sentence was not copied.

[80.] Nm/Fragment 072 27

Verschleierung

Untersuchte Arbeit: Seite: 72, Zeilen: 27-32	Quelle: Arquilla_Ronfeldt_2001 Seite(n): 72, Zeilen: 16ff	Farbig
2.9.6 Network Cores	**Network Cores**	
Networks of any significant size will generally have a central / core and a periphery/ foot soldier, reflecting asymmetries of power, influence, and status within the network. The central member is characterized by dense connections among individuals who, in the case of a directed network, provide the steering mechanism for the [network as a whole.]	Networks of any substantial size will generally have both a core and a periphery, reflecting asymmetries of power, influence, and status within the network. The core is characterized by dense connections among individuals who, in the case of a directed network, provide the steering mechanism for the network as a whole.	

Anmerkungen

Slight adaptations. The source is not referenced

[81.] Nm/Fragment 073 01

Verschleierung

Untersuchte Arbeit: Seite: 73, Zeilen: 1-31	Quelle: Arquilla_Ronfeldt_2001 Seite(n): 72-73, Zeilen: 21ff, 1ff	Farbig

Usually the originators of the criminal enterprise, the central members initiate specific criminal activities, arbitrate disputes, and provide direction. Their relationship is often supported by bonding mechanisms that help to create high degrees of trust and cohesion.

In many cases, bonding will be directly related to family or kinship: For example, many Italian Mafia groups are still organized along family lines, while Turkish drug trafficking and criminal organizations are often clan based. Other bonding mechanisms include ethnicity and common experience in which the participants develop a strong sense of trust and mutual reliance.

Membership in youth gangs or time spent together in prison can also provide critical bonding mechanisms. In the United States, the Mexican Mafia (which is not actually Mexican) started as a prison gang in Southern California but has developed much more extensively. Yet, it is the common experience that continues to provide the network core with the capacity to operate with confidence and believe that disloyalty or defection is very unlikely.

If network cores exhibit strong collective identities, cohesion does not necessarily enhance—and can actually reduce—the capacity to obtain information and "mobilize resources from the environment." Indeed, recent trends in network analysis posit an inverse relationship, in general, between the density/intensity of the coupling of network ties on the one hand and their openness to the outside environment on the other (Grabher, G., Stark, D., 1997)

This explains the attraction of a two-tier structure in which the weaknesses of the central member in carrying out the functions of information acquisition are more than offset by the foot soldiers/ peripheries.

2.9.7 Network Peripheries

The peripheries feature less dense patterns of interaction and looser [relationships than the core.]

Usually the originators of the criminal enterprise, the core members initiate specific criminal activities, arbitrate disputes, and provide direction. Their relationship is often underpinned by bonding mechanisms that help to create high degrees of trust and cohesion.

In many cases, bonding will be directly related to family or kinship: Many Italian Mafia groups are still organized along family lines, while Turkish drug trafficking and criminal organizations are often clan based. Other bonding mechanisms include ethnicity and common experience in which the participants develop a strong sense of trust and mutual reliance.

Membership in youth gangs or time spent together in prison can also provide critical bonding mechanisms. In the United States, the Mexican Mafia (which is not actually Mexican) started as a prison gang in

[Page 73]

Southern California but has developed much more extensively. Yet, it is the common experience that continues to give the core of the network a capacity to operate with confidence that disloyalty or defection are unlikely.[FN 15]

If network cores exhibit strong collective identities, cohesion does not necessarily enhance—and can actually reduce—the capacity to obtain information and "mobilize resources from the environment." Indeed,

> recent trends in network analysis posit an inverse relationship, in general, between the density/intensity of the coupling of network ties on the one hand and their openness to the outside environment on the other.[FN 16]

This explains the attraction of a two-tier structure in which the weaknesses of the core in carrying out the functions of information acquisition are more than offset by the periphery.

Network Peripheries

This zone features less dense patterns of interaction and looser relationships than the core.

[FN 15] The analysis here and the discussion of bonding mechanisms rests heavily on Ianni, 1974, pp.282-293.

[FN 16] See David Stark and Gernot Grabher, "Organizing Diversity: Evolutionary Theory, Network Analysis, and Postsocialist Transformations," in Stark and Grabher, eds., Restructuring Networks: Legacies, Linkages, and Localities in Postsocialism (New York and London: Oxford University Press, in press).

Anmerkungen

Very minor adaptations. The source is not given.

One literature reference has been removed, another reference for a quote has been taken from the source, and the period was omitted after the inserted reference.

[82.] Nm/Fragment 074 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 74, Zeilen: 1-7	Quelle: Arquilla_Ronfeldt_2001 Seite(n): 73, Zeilen: 18ff	Farbig
Yet, these characteristics play a critical role in networks, exhibiting and exploiting "the strength of weak ties" (Granovetter, M., 1973). In effect, the periphery allows the network to operate at a far greater distance, both geographically and socially, than would otherwise be the case. Thus it facilitates more-extensive operations, more-diverse activities, and the capacity to carry out effective intelligence collection.	Yet, these characteristics play a critical role in networks, exhibiting and exploiting "the strength of weak ties." [FN 17] In effect, the periphery allows the network to operate at a far greater distance —both geographically and socially— than would otherwise be the case, facilitating more-extensive operations, more-diverse activities, and the capacity to carry out effective intelligence collection. [FN 18] [FN 17] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology*, Vol. 78 (1973) pp. 1360-1380. [FN 18] Ibid. and Burt, 1992.	

Anmerkungen

Only very slight adaptations. The source is not given.

Note that also one literature reference is taken from the source (and another has been removed).

Note also the identical usage of the words "more-extensive" and "more-diverse".

[83.] Nm/Fragment 074 08

Verschleierung

Untersuchte Arbeit: Seite: 74, Zeilen: 8-30	Quelle: Lemieux_2003 Seite(n): 6, 12, Zeilen: page 6: 1-2, 9-17 ; page 12: 2-5	Farbig
2.9.8 Size of Networks Size is a fundamental characteristic of networks. It determines many other characteristics including link density, commonly called as density of the network. Generally, density is higher in a small network than in a large one. It is because in a large network, a large proportion of connections between participants are indirect. This is the case for transnational criminal networks, which were specifically studied by Williams and his collaborators (Williams, 2001; Williams and Godson, 2002). Williams states that these networks can be considered to be composed of strategic alliances between national networks, e.g., the Columbian drug trade network and the Sicilian drug distribution network. There are also large networks within a single country. Generally, they are made up of subset of the main networks among which there are loose couplings through weak ties, particularly important in criminal networks. 2.9.9 Redundancy in Networks The link density of a network increases, if several actors or ties must be removed to break it into unconnected pieces making it more redundant. As stated by Williams (2001) "…redundancy enables members of the network to take over tasks and responsibilities from those who have been arrested, incarcerated, or [killed by law enforcement."]	Size of the Networks Size is a fundamental characteristic of networks, in that it determines many other characteristics, particularly the density of the networks. [...] Generally, density is higher in a small network than in a large one, meaning that, in a large network, a large proportion of connections between participants are indirect. This is the case for transnational criminal networks, which were specifically studied by Williams and his collaborators (Williams, 2001; Williams and Godson, 2002). Williams states that these networks can be considered to be composed of strategic alliances between national networks, e.g., the Columbian drug trade network and the Sicilian drug distribution network. There are also large networks within a single country. Generally, they are made up of subnetworks between which there are loose couplings through weak ties, particularly important in criminal networks. [...][Page 12] A network is even more redundant and, thus, denser, if several actors or ties must be removed to break it into pieces that are not connected. As stated by Williams (p. 81) " … redundancy enables members of the network to take over tasks and responsibilities from those who have been arrested, incarcerated, or killed by law enforcement."	

Anmerkungen

Minor Adjustments. The source is not given anywhere in the thesis.

[84.] Nm/Fragment 075 07

Verschleierung

Untersuchte Arbeit: **Seite: 75, Zeilen: 7-25**	**Quelle: Xu and Chen 2005a** **Seite(n): 102, Zeilen: left column 53 - right column 1-21** Farbig
First, incomplete, incorrect, or inconsistent data can create problems. Moreover, these characteristics of terrorist networks cause difficulties: -**Incompleteness**. Criminal networks are clandestine networks that work in concealment and secrecy (Krebs, 2002). Criminals may reduce communications to avoid attracting attention of law enforcement agencies and their communications are concealed behind a number of illegal activities. Therefore, data about criminal networks is certainly treated as incomplete; that is, some existing links or nodes will be overlooked or unrecorded (Sparrow, M. K., 1991). -**Incorrectness**. Many criminals hide their identity (provide incorrect information to the agencies) when they are captured and under investigation. Incorrect data regarding criminals' identities, physical characteristics, and addresses may result either from accidental data entry errors or from intentional cheating by criminals. -**Inconsistency**. Information about criminals, who have captured a number of times at number of places, may be entered in law [enforcement databases multiple times.]	First, incomplete, incorrect, or inconsistent data can create problems. Moreover, these characteristics of criminal networks cause difficulties not common in other data mining applications: • *Incompleteness*[EN 10]. Criminal networks are covert networks that operate in secrecy and stealth [EN 8]. Criminals may minimize interactions to avoid attracting police attention and their interactions are hidden behind various illicit activities. Thus, data about criminals and their interactions and associations is inevitably incomplete, causing missing nodes and links in networks [EN 10]. • *Incorrectness*. Incorrect data regarding criminals' identities, physical characteristics, and addresses may result either from unintentional data entry errors or from intentional deception by criminals. Many criminals lie about their identity information when caught and investigated. • *Inconsistency*. Information about a criminal who has multiple police contacts may be entered into law enforcement databases multiple times. [EN 8] Krebs, V. E. Mapping networks of terrorist cells. *Connections* 24, 3 (2001), 43–52. [EN 10] Sparrow, M.K. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13 (1991), 251–274.

Anmerkungen

Starts out as "word-for-word paraphrasing" and becomes "word-for-word copying" (even more obvious on the next page). The source is not given

If indeed there is an article where "Most part of the contents of this subsection is already published in (Memon N., and Larsen H. L., 2006a).", as Nm claims in the footnote, one has to wonder about the refereeing process there, too.

[85.] Nm/Fragment 076 01

Verschleierung

Untersuchte Arbeit: **Seite: 76, Zeilen: 1-17, 20-25, 29-32**	**Quelle: Xu and Chen 2005a** **Seite(n): 102, Zeilen: right column 19ff**
[Information about criminals, who have captured a number of times at number of places, may be entered in law] enforcement databases multiple times. These records are not unsurprisingly consistent. It would be found very strange if multiple data records could make a single criminal appear to be different individuals. When apparently different individuals are included in a network under investigation, misleading information may be produced.	Information about a criminal who has multiple police contacts may be entered into law enforcement databases multiple times. These records are not necessarily consistent. Multiple data records could make a single criminal appear to be different individuals. When seemingly different individuals are included in a network under study, misleading information may result.
The literature study found that the problems particularly to criminal network analysis lie in data transformation, fuzzy boundaries, and network dynamics.	Problems specific to criminal network analysis lie in data transformation, fuzzy boundaries, and network dynamics:
-**Data Transformation**. Network analysis requires that data be presented in a particular format, in which (network) members' represent nodes, their communications are represented by links. Though, information about criminal relations is typically not precise in raw data and converting them to the required format can be known as laborious and time-consuming.	• *Data transformation*. Network analysis requires that data be presented in a specific format, in which network members are represented by nodes, and their associations or interactions are represented by links. However, information about criminal associations is usually not explicit in raw data. The task of extracting criminal associations from raw data and transforming them to the required format can be fairly labor-intensive and time-consuming.
-**Fuzzy boundaries**. The boundaries of criminal networks are relatively confusing. [...] Therefore, it is found during the literature review that it can be very tough for an analyst to choose whom to include and whom to exclude from a network under investigation (Sparrow, M. K., 1991).	• Fuzzy boundaries. Boundaries of criminal networks are likely to be ambiguous. It can be quite difficult for an analyst to decide whom to include and whom to exclude from a network under study [EN 10].
-**Dynamic**. Criminal networks are known as dynamic networks, that is, they usually to change over time. {The relationship between any two individuals binary nature, it means there is a relation or there is no relation, it may be weak or strong; rather it has a distribution over time, waxing and waning from one period to another. It is also noted that most of relations change in time.} Therefore, it is need of the time to design and develop new methods of data collection in order to capture the dynamics of criminal networks (Sparrow, M. K., 1991).	• Network dynamics. Criminal networks are not static, but are subject to changes over time. New data and even new methods of data collection may be required to capture the dynamics of criminal networks [EN 10].

Farbig

Anmerkungen

Text between line 25 and line 29 (marked by {}) seems to be Nm's own. It is left as an example of Nm's style in comparison to the original own. (These lines are not counted).

[86.] Nm/Fragment 077 03

BauernOpfer

Untersuchte Arbeit: **Seite: 77, Zeilen: 3-29**	**Quelle: Xu and Chen 2005a** **Seite(n): 103, Zeilen: left column 16-52** Farbig
Criminal Network Analysis, which is a broad category of terrorist network analysis, can be categorized into three generations (Xu J., Chen H., 2006):	Klerks [EN 7] categorized existing criminal network analysis approaches and tools into three generations.
First generation: Manual approach. The representation of first generation is known as Anacapa chart (Klerks, 2001). Using this approach, an analyst should first develop an association matrix by detecting criminal associations from raw data. Then, a link chart for visualization purposes can then be drawn based on the association matrix. For example, to map the terrorist network containing the 19 hijackers in 9/11 attacks, Krebs (Krebs, 2002) gathered data about the relationships among the hijackers from publicly available information reported in several major newspapers. Krebs then manually constructed an association matrix to incorporate these relations (Krebs, 2002) and illustrated a network representation in order to analyze the structural properties of the network.	**First generation: Manual approach**. Representative of the first generation is the Anacapa Chart [EN 6]. With this approach, an analyst must first construct an association matrix by identifying criminal associations from raw data. A link chart for visualization purposes can then be drawn based on the association matrix. For example, to map the terrorist network containing the 19 hijackers in the September 11 attacks, Krebs [EN 8] gathered data about the relationships among the hijackers from publicly released information reported in several major newspapers. He then manually constructed an association matrix to integrate these relations [EN 8] and drew a network representation to analyze the structural properties of the network (Figure 1).
It is well known fact that such a manual approach for criminal network analysis is helpful in crime investigation; but this type of approach is would be good if the dataset is short, but it would be difficult rather impossible to draw a link chart if there are thousands of nodes.	Although such a manual approach for criminal network analysis is helpful in crime investigation, it becomes an extremely ineffective and inefficient method when data sets are very large.
Second generation: Graphic-based approach. These tools can automatically produce graphical representations of criminal networks. Most of the available network analysis tools belong to this generation. Among them Analyst's Notebook, Netmap and XANALYS Link Explorer (previously called Watson) are the most popular (Xu, J., Chen H., 2006). It is to mention that, Analyst's Notebook (see Figure 2.3) can automatically generate a link chart [based on relational data from a spread sheet or text file.]	**Second generation: Graphic-based approach.** These tools can automatically produce graphical representations of criminal networks. Most existing network analysis tools belong to this generation. Among them Analyst's Notebook [EN 7], Netmap [EN 5], and XANALYS Link Explorer (previously called Watson) [EN 1], are the most popular. For example, Analyst's Notebook can automatically generate a link chart based on relational data from a spreadsheet or text file (Figure 2a).
	[EN 1] Anderson, T., Arbetter, L., Benawides, A., and Longmore-Etheridge, A. Security works. *Security Management* 38, 17, (1994), 17–20.
	[EN 5] Goldberg, H.G., and Senator, T.E. Restructuring databases for knowledge discovery by consolidation and link formation. In *Proceedings of 1998 AAAI Fall Symposium on Artificial Intelligence and Link Analysis*. AAAI Press (1998).
	[EN 6] Harper, W.R., and Harris, D.H. The application of link analysis to police intelligence. *Human Factors* 17, 2 (1975), 157–164.
	[EN 7] 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 (2001), 53–65.
	[EN 8] Krebs, V. E. Mapping networks of terrorist cells. *Connections* 24, 3 (2001), 43–52.

Anmerkungen

Source is given at the beginning, but nothing has been marked as a citation.

Again "Most of the parts of the contents of this subsection are already published in (Memon N., and Larsen H. L., 2006a)."

[87.] Nm/Fragment 078 01

Verschleierung

Farbig

Untersuchte Arbeit: **Seite: 78, Zeilen: 1-13**	**Quelle: Xu and Chen 2005a** **Seite(n): 103, Zeilen: left column 49-52 and right column 14-28**
[It is to mention that, Analyst's Notebook (see Figure 2.3) can automatically generate a link chart] based on relational data from a spread sheet or text file.	For example, Analyst's Notebook can automatically generate a link chart based on relational data from a spreadsheet or text file (Figure 2a).
Though second generation tools are capable of using a number of methods to visualize criminal networks, their sophistication level is not up to the mark because they only produce graphical representation of criminal networks with less analytical functionality. These tools still rely on analysts to investigate the graphs with awareness to detect structural properties of the network.	Although second-generation tools are capable of using various methods to visualize criminal networks, their sophistication level remains modest because they produce only graphical representations of criminal networks without much analytical functionality. They still rely on analysts to study the graphs with awareness to find structural properties of the network.
[...]	[...]
Third generation: SNA. This generation provides more advanced functionality to help the law enforcement professionals in crime investigations. Complex structural analysis tools are needed to visualization facility in addition of mining large amount of data in order to discover useful knowledge about the structure and organization of criminal networks.	**Third generation: SNA**. This approach is expected to provide more advanced analytical functionality to assist crime investigation. Sophisticated structural analysis tools are needed to go from merely drawing networks to mining large volumes of data to discover useful knowledge about the structure and organization of criminal networks.

Anmerkungen

continuation from previous page

[88.] Nm/Fragment 079 03

Verschleierung

Untersuchte Arbeit: Seite: 79, Zeilen: 3-18	Quelle: Xu etal 2004 Seite(n): 3, Zeilen: 5-13
A terrorist network is primarily a social network in which individuals connect with one another through various connections such as kinship, friendship, colleagues, and classmates, etc. Research has recognized SNA as a promising methodology to analyze the structural properties of criminal/ terrorist networks (Krebs, V., 2002; McAndrew, D., 1999 Sparrow, M.K., 1991). SNA was originally used in sociology research to extract patterns of relationships between social actors in order to discover the underlying social structure (Wasserman, S. and K. Faust, 1994; Wellman, B., 1988). A social network is often known as a graph in which nodes (or actors) represent individual members and links (or connections) represent relations among the members. The sructural properties of a social network can be described and analyzed at four levels: node, link, group, and overall network. SNA provides various measures, indexes, and approaches to capture these structural properties quantitatively.	A criminal network is primarily a social network in which individuals connect with one another through various relations such as kinship, friendship, and co-workers. Research has recognized SNA as a promising methodology to analyze the structural properties of criminal networks [EN 23, EN 26, EN 35]. SNA was originally used in sociology research to extract patterns of relationships between social actors in order to discover the underlying social structure [EN 38, EN 39]. A social network is often treated as a graph in which nodes represent individual members and links represent relations among the members. The structural properties of a social network can be described and analyzed at four levels: node, link, group, and the overall network. SNA provides various measures, indexes, and approaches to capture these structural properties quantitatively. --- [EN 23] Krebs, V.E. (2001). Mapping networks of terrorist cells. *Connections, 24(3),* 43-52. [EN 26] McAndrew, D. (1999). The structural analysis of criminal networks, in *The social psychology of crime: Groups, teams, and networks, offender profiling series, iii,* D. Canter & L. Alison (eds.). Aldershot: Dartmouth. [EN 35] Sparrow, M.K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13,* 251-274. [EN 38] Wasserman, S. & K. Faust (1994). *Social network analysis: Methods and applications*, ed. Series. Cambridge: Cambridge University Press. [EN 39] Wellman, B. (1988). Structural analysis: From method and metaphor to theory and substance, in *Social structures: A network approach*, B. Wellman & S.D. Berkowitz (eds.). Cambridge University Press: Cambridge.

Farbig

Anmerkungen

Only minor adaptations. All literature references have been copied as well. The source is not given

[89.] Nm/Fragment 079 19

Verschleierung

Untersuchte Arbeit: Seite: 79, Zeilen: 19-29	Quelle: Clark etal 2005 Seite(n): 4, Zeilen: 7-14
Researchers (for example; Simmel, 1906; Gross, 1980; Geis and Stotland, 1980; Erickson, 1981; Baker and Faulkner, 1993; Klerks, 2001) have conducted psychological and sociological analyses of covert networks for the past century, however since Sept. 11, 2001 there has been a dramatic increase in the number of publications (ex. Krebs, 2001; Carley et al, 2003, Sageman, 2004) on covert networks, specifically terror networks. These recent researchers have chosen Social Network Analysis (SNA) to help them “map,” (Krebs, 2001) “uncloak,” (Krebs, 2002) “identify key players,” (Borgatti, 2002) “destabilize,” (Carley et al., 2003) and “understand” (Sageman, 2004) terror networks.	Researchers (ex. Simmel, 1906; Gross, 1980; Geis and Stotland, 1980; Erickson, 1981; Baker and Faulkner, 1993; Klerks, 2001) have conducted analyses of clandestine networks for the past century, however since Sept. 11, 2001 there has been a dramatic increase in the number of publications (ex. Krebs, 2001; Carley et al, 2003, Sageman, 2004) on clandestine networks, specifically terror networks. These recent researchers have chosen SNA to help them "map," (Krebs, 2001) "uncloak," (Krebs, 2002) "identify key players," (Borgatti, 2002) "destabilize," (Carley et al., 2003) and "understand" (Sageman, 2004) terror networks.

Farbig

Anmerkungen

No source given

[90.] Nm/Fragment 080 01

Verschleierung

Untersuchte Arbeit:
Seite: 80, Zeilen: 1-29

There have been some empirical studies that have used SNA methods to analyze criminal or terrorist networks. For instance, based on archival data, Baker and Faulkner analyzed the structure of an illegal network depicting a price-fixing conspiracy in the heavy electrical equipment industry. Their findings supported that individual centrality in the network, as measured by degree, betweenness, and closeness (Freeman, L.C., 1979), was an important forecaster of an individual's possible prosecution (Baker, W.E. and R.R. Faulkner 1993). Krebs analysed the open source data and studied the terrorist network involved in 9/11 terrorist plot. He found that *Mohamed Atta*, who piloted the first plane that crashed into the World Trade Center, had the highest degree and acted as the ring leader of the network (Krebs, V., 2002). Xu and Chen employed clustering, centrality measures, block-modeling,and multidimensional scaling (MDS) approaches from SNA to study criminal networks based on crime incident data (Xu, J. & H. Chen, 2003). The system they developed can also visualize a network and its groups.

In the following section we review related SNA research about dynamic network analysis and visualization.

2.13 ANALYZING SOCIAL NETWORK DYNAMICS

Recently, the attention on research on social network dynamics has increased. However, there has not been a consensus on what analytical methods to use (Carley, K.M., *et al*., 2003; Doreian, P., *et al*., 1997; Nakao, K. and A.K. Romney, 1993). Research uses various methods, measures, models, and techniques to studynetwork dynamics. Doreian and Stokman classified existing approaches into three categories: descriptive, statistical, andsimulation methods (Doreian, P. and F.N. Stokman, 1997).

Quelle: Xu etal 2004
Seite(n): 3-4, Zeilen: 3:14ff; 4:11-22

Farbig

There have been some empirical studies that use SNA methods to analyze criminal or terrorist networks. For instance, based on archival data, Baker and Faulkner analyzed the structure of an illegal network depicting a price-fixing conspiracy in the heavy electrical equipment industry. They find that individual centrality in the network, as measured by degree, betweenness, and closeness [EN 17], is an important predictor of an individual's possible prosecution [EN 1]. Krebs relied on open source data and studied the terrorist network centering around the 19 hijackers in 9/11 events. He found that Mohamed Atta, who piloted the first plane that crashed into the World Trade Center, had the highest degree and acted as the ring leader of the network [EN 23]. Xu and Chen employed clustering, centrality measures, blockmodeling, and

[P. 4]

multidimensional scaling (MDS) approaches from SNA to study criminal networks based on crime incident data [EN 41]. The system they developed can also visualize a network and its groups.

[...]

3. Literature Review

In this section we review related SNA research about dynamic network analysis and visualization.

3.1 Analyzing social network dynamics

Recently, the research on social network dynamics has received increasing attention. However, there has not been a consensus on what analytical methods to use [EN 4, EN 14, EN 27]. Research uses various methods, measures, models, and techniques to study network dynamics. Doreian and Stokman classified existing approaches into three categories: descriptive, statistical, and simulation methods [EN 15].

[Pp. 27-29]

[EN 1] Baker, W.E. & R.R. Faulkner (1993) The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review*, 58(12), 837-860.

[EN 4] Carley, K.M., et al. (2003) Destabilizing dynamic covert networks. In Proceedings of the *8th International Command and Control Research and Technology Symposium*. Washington DC., VA.

[EN 14] Doreian, P., et al. (1997) A brief history of balance through time, in *Evolution of social networks*, P. Doreian & F.N. Stokman (eds.). Gordon and Breach: Australia. 129-147.

[EN 15] Doreian, P. & F.N. Stokman (1997) The dynamics and evolution of social networks, in *Evolution of social networks*, P. Doreian & F.N. Stokman (eds.). Gordon and Breach: Australia. 1-17.

[EN 17] Freeman, L.C. (1979). Centrality in social networks: Conceptual clarification. *Social Networks*, 1, 215-240.

[EN 23] Krebs, V.E. (2001). Mapping networks of terrorist cells. *Connections*, 24(3), 43-52.

[EN 27] Nakao, K. & A.K. Romney (1993) Longitudinal approach to subgroup formation: Re-analysis of Newcomb's fraternity data. *Social Networks*, 15, 109-131.

[EN 41] Xu, J. & H. Chen (2003). Untangling criminal networks: A case study. In *Proceedings of NSF/NIJ Symposium on Intelligence and Security Informatics (ISI'03)* Tucson, AZ.

Anmerkungen

Source is not given. The text has been copied with only minor adjustments -- also all literature references have been copied.

[91.] Nm/Fragment 081 01

Verschleierung

Untersuchte Arbeit: **Seite: 81, Zeilen: 1-32**	**Quelle: Xu etal 2004** **Seite(n): 5, Zeilen: 1ff**
2.13.1 Descriptive methods	*3.1.1 Descriptive methods*
The descriptive analysis is often employed to detect structural changes in social networks. Desciptive methods are used to test how well a sociologic theory is supported by empirical data. With descriptive methods, structural properties of a social network are measured by various metrics and indexes and compared across time to describe the dynamics in nodes, links, or groups in the network. Little research has been found that studied the dynamics at the overall network level.	The purpose of descriptive analysis is often to detect structural changes in social networks and test how well a sociologic theory is supported by empirical data. With descriptive methods, structural properties of a social network are measured by various metrics and indexes and compared across time to describe the dynamics in nodes, links, or groups in the network. Little research has been found which studied the dynamics at the overall network level.
Node level measures and values often focus on and reflect the changes in individuals' centrality, influence, and other characteristics in a social network. To study how an individual's social position relates to his or her technology adoption behavior, Burkhardt and Brass studied a communication network of 94 employees of an organization at four time points after a new computerized information system was deployed (Burkhardt, M.E. and D.J. Brass, 1990).	Node level measures often focus on changes in individuals' centrality, influence, and other characteristics. To study how an individual's social position relates to his or her technology adoption behavior, Burkhardt and Brass studied a communication network of 94 employees of an organization at four time points after a new computerized information system was deployed [EN 3]. They found that the centrality (degree and closeness) and power of early adopters of new technology increased over time. Using Newcomb's classic longitudinal data [EN 28], Nakao and Romney measured the "positional stability" of 17 new members in a fraternity during a 15-week period [EN 27]. For each week, these individuals were mapped into a two-dimensional MDS diagram based on their relational strength. As individuals may change their positions over time, the lengths of their paths of movement were calculated with a short path indicating a high positional stability. The positional stability index was used to examine how popular and unpopular individuals differ in the speed with which they found their appropriate social groups. In the area of citation analysis where an author citation network is treated as a social network, centrality type metrics have been used to trace the dynamics of authors' influence on a scientific discipline.
They found that the centrality (degree and closeness) and power of early adopters of new technology increased over time. Using Newcomb's classic longitudinal data (Newcomb, T.M., 1961), Nakao and Romney measured the "positional stability" of 17 new members in a fraternity during a 15-week period (Nakao, K. and A.K. Romney, 1993). For each week, these individuals were mapped into a two-dimensional MDS diagram based on their relational strength. As individuals may change their positions over time, the lengths of their paths of movement were calculated with a short path indicating a high positional stability.	
The positional stability index was used to examine how popular and unpopular individuals differ in the speed with which they found their appropriate social groups. In the area of citation analysis where an author citation network is treated as a social network, centrality type metrics have been used to trace the [dynamics of authors' influence on a scientific discipline.]	

[EN 3]. Burkhardt, M.E. & D.J. Brass (1990). Changing patterns or patterns of change: The effects of a change in technology on social network structure and power. *Administrative Science Quarterly*, 35, 104-127.

[EN 27]. Nakao, K. & A.K. Romney (1993). Longitudinal approach to subgroup formation: Re-analysis of Newcomb's fraternity data. *Social Networks*, 15, 109-131.

[EN 28]. Newcomb, T.M. (1961). *The acquaintance process*, ed. Series. New York: Holt, Rinehart, & Winston.

Anmerkungen

Only minor adjustments. Also literature references have been copied. Source is not given.

[92.] Nm/Fragment 082 01

Verschleierung

Untersuchte Arbeit: **Seite: 82, Zeilen: 1-32**	**Quelle: Xu etal 2004** **Seite(n): 5, 6, Zeilen: 5: 21ff; 6:1ff** Farbig
For example, an author citation network in information science during 1972-1995 was studied in (White, H.D. and K.W. McCain, 1998). A centrality index was calculated based on an author's mean number of co-citations with other authors. This index was used to reflect the changes in the author's influence over time.	For example, an author citation network in information science during 1972-1995 was studied in [EN 40]. A centrality index is calculated based on an author's mean number of co-citations with other authors. This index is used to reflect the changes in the author's influence over time.
Link stability has also been researched in various case studies, especially inter-organizational network studies. It is the rate of link breaking and replacement. For example, Ornstein examined the interlocking relations among the 100 largest Canadian companies between 1946-1977 (Ornstein, M.D., 1982). He calculated the percentage of relations that were previously broken but later restored and used in order to test whether the network was dominated by planned liaisons. Similarly, Fennema and Schijf used "chance of restoration" to identify a stable set of interlocking relations among companies across several countries (Fennema, M. and H. Schijf, 1978/79).	[Page 6] Link stability in terms of link breaking and replacement rate was analyzed in several inter-organizational network studies. Ornstein examined the interlocking relations among the 100 largest Canadian companies between 1946-1977 [EN 30]. He calculated the percentage of relations that were previously broken but later restored and used that to test whether the network was dominated by planned liaisons. Similarly, Fennema and Schijf used "chance of restoration" to identify a stable set of interlocking relations among companies across several countries [EN 16].
Research has focused on group stability and group balance processes to describe group level dynamics. To analyze group balance processes, Doreian and Kapuscinski used Newcomb's fraternity data (Newcomb, T.M., 1961) to measure relation reciprocity, transitivity, and imbalance across the 15 weeks (Doreian, P., et al.., 1997). Results for each week were then plotted to study the trend of group balance over time. Group stability is defined in Nakao and Romney's study as the similarity between the two socio-metrics representing the same group at two different points of time (Nakao, K. and A.K. Romney, 1993). In citation analysis, "Cluster Stability Index" is proposed. It is defined as the number of common elements in two clusters divided by the total number of elements in the two clusters (Small, H.G., 1977). By calculating this index between two similar clusters in two successive time periods, it is [possible to measure the stability or continuity of a scientific field as represented by a group of authors (Braam, R.R., H.F. Moed, and A.F.J. van Raan, 1991).]	To describe group level dynamics, research has focused on group stability and group balance processes. To analyze group balance processes, Doreian and Kapuscinski used Newcomb's fraternity data [FN 28] to measure relation reciprocity, transitivity, and imbalance across the 15 weeks [FN 14]. Results for each week were then plotted to study the trend of group balance over time. Group stability is defined in Nakao and Romney's study as the similarity between the two sociomatrices representing the same group at two different points of time [EN 27]. In citation analysis, Small proposes a "Cluster Stability Index", which is defined as the number of common elements in two clusters divided by the total number of elements in the two clusters [EN 32]. By calculating this index between two similar clusters in two successive time periods, it is possible to quantify the stability or continuity of a scientific field as represented by a group of authors [EN 2].

[EN 2] Braam, R.R., H.F. Moed, & A.F.J. van Raan (1991). Mapping of science by combined co-citation and word analysis ii: Dynamical aspects. *Journal of American Society of Information Science*, 42(4), 252-266.

[EN 14] Doreian, P., et al. (1997) A brief history of balance through time, in *Evolution of social networks*, P. Doreian & F.N. Stokman (eds.). Gordon and Breach: Australia. 129-147.

[EN 16] Fennema, M. & H. Schijf (1987/79). Analyzing interlocking directories: Theory and methods. *Social Networks*, 1, 297-332.

[EN 17] Freeman, L.C. (1979). Centrality in social networks: Conceptual clarification. *Social Networks*, 1, 215-240.

[EN 27] Nakao, K. & A.K. Romney (1993) Longitudinal approach to subgroup formation: Re-analysis of Newcomb's fraternity data. *Social Networks*, 15, 109-131.

[EN 28] Newcomb, T.M. (1961). *The acquaintance process*, ed. Series. New York: Holt, Rinehart, & Winston.

[EN 30] Ornstein, M.D. (1982). Interlocking directorates in Canada: Evidence from replacement patterns. *Social Networks*, 4, 3-25.

[EN 32] Small, H.G. (1977). A co-citation model of a scientific specialty: A longitudinal study of collagen research. *Social Studies of Science*, 7, 139-166.

[EN 40] White, H.D. & K.W. McCain (1998). Visualizing a discipline: An author co-citation analysis of information science, 1972-1995. *Journal of American Society of Information Science and Technology*, 49(4), 327-355.

Anmerkungen

In the same style as on the previous pages: only minor adjustments, all literature references are copied as well, and the source is not mentioned.

[93.] Nm/Fragment 083 01

Verschleierung

Untersuchte Arbeit: Seite: 83, Zeilen: 1-3	Quelle: Xu_etal_2004 Seite(n): 6, Zeilen: 15-17
[By calculating this index between two similar clusters in two successive time periods, it is] possible to measure the stability or continuity of a scientific field as represented by a group of authors (Braam, R.R., H.F. Moed, and A.F.J. van Raan, 1991).	By calculating this index between two similar clusters in two successive time periods, it is possible to quantify the stability or continuity of a scientific field as represented by a group of authors [2]. [2]. Braam, R.R., H.F. Moed, & A.F.J. van Raan (1991). [...]

Farbig

Anmerkungen

Continued from previous page

[94.] Nm/Fragment 083 04

Verschleierung

Untersuchte Arbeit: Seite: 83, Zeilen: 4-30	Quelle: CNS_2002 Seite(n): 80, 95, 172, Zeilen: 80: 7ff; 95: 12ff; 172: 10ff
Valdis Krebs [FN 12] worked in analyzing organizations, especially adaptive organizations. He has applied real-world data and model “social network processes”. He has done some work on analyzing the terrorist network surrounding the 9/11 attacks (Krebs, V.; 2001, 2002). He states that one can also apply his analysis to counterterrorist organization and believes it takes a network to fight a network; he therefore prescribes the use of small anti-terror teams. In his approach, Krebs (2002) takes a snapshot of a network. After many such snapshots, he can see how networks evolve. He argues that one can see patterns at the planning stage of terrorist attacks - a terrorist planning team looks like any other planning team. So, once they get into active planning mode, terrorists’ project map looks like anyone else’s. One can use this knowledge to analyze groups and see where they are in the operational process. Krebs (2002) also emphasizes that terrorists, like other organizations, do have leaders, so one does not necessarily need all the data – we can obtain a lot of information without it. There has been a great deal of work in link analysis in law enforcement. Link analysis focuses more on objects and people, whereas Krebs’ software concentrates on people and uses social network metrics. Roger Smith (Smith, R., 2001) presented a definition of social cohesion based on network connectivity that leads to an operationalization of social embeddedness. He defined cohesiveness as the minimum number of actors who, if removed from a group, would disconnect the group. Borgatti Stephen P. (2003) discussed how to identify sets of structurally key players, particularly in the context of attacking [terrorist networks.] [FN 12] http://www.orgnet.com/VKbio.html	- Mr. Krebs works in analyzing organizations, especially adaptive organizations. He would like to apply what he does to real-world data and model ‘social network processes’. - He has done some work on analyzing the terrorist network surrounding the 9/11 attacks. He states that one can also apply his analysis to counterterrorist organization and believes it takes a network to fight a network; he therefore prescribes the use of small anti-terror teams. - In his approach, Mr. Krebs takes a snapshot of a network. After many such snapshots, he can see how networks evolve. He argues that one can see patterns at the planning stage of terrorist attacks - a terrorist planning team looks like any other planning team. So, once they get into active planning mode, terrorists’ project map looks like anyone else’s. One can use this knowledge to analyze groups and see where they are in the operational process. Mr. Krebs also emphasizes that terrorists, like other organizations, do have leaders, so one does not necessarily need all the data – we can obtain a lot of information without it. - There has been a lot of work in link analysis in law enforcement. Link analysis focuses more on objects and people, whereas Mr. Krebs’ software concentrates on people and uses social network metrics. [page 95] We present a definition of social cohesion based on network connectivity that leads to an operationalization of social embeddedness. We define cohesiveness as the minimum number of actors who, if removed from a group, would disconnect the group. [page 172] This paper discusses how to identify sets of structurally key players, particularly in the context of attacking terrorist networks.

Farbig

Anmerkungen

The given internet link does (and did not) give the same information let alone in the same formulations as the source.

[95.] Nm/Fragment 084 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 84, Zeilen: 1-10	Quelle: CNS_2002 Seite(n): 172, Zeilen: 10-16
[Borgatti Stephen P. (2003) discussed how to identify sets of structurally key players, particularly in the context of attacking] terrorist networks. Three specific goals are discussed: (a) identifying nodes whose deletion would maximally fragment the network, (b) identifying nodes that, based on structural position alone, are potentially “in the know”, and (c) identifying nodes that are in a position to influence others. Measures of success, in the form of fragmentation and reach indices, are developed and used as cost functions in a combinatorial optimization algorithm. The algorithm is compared against naïve approaches based on choosing the k most central players, as well as against approaches based on group centrality.	This paper discusses how to identify sets of structurally key players, particularly in the context of attacking terrorist networks. Three specific goals are discussed: (a) identifying nodes whose deletion would maximally fragment the network, (b) identifying nodes that, based on structural position alone, are potentially “in the know”, and (c) identifying nodes that are in a position to influence others. Measures of success, in the form of fragmentation and reach indices, are developed and used as cost functions in a combinatorial optimization algorithm. The algorithm is compared against naïve approaches based on choosing the k most central players, as well as against approaches based on group centrality.

Farbig

Anmerkungen

The source is not given. The copied text starts on the previous page.

[96.] Nm/Fragment 084 11

Verschleierung

Untersuchte Arbeit: Seite: 84, Zeilen: 11-33	Quelle: Berry_etal_2004 Seite(n): 1, 2, Zeilen: 1: left column, Abstract; right column 19; 2: left column 1
Berry, Nina *et al* (2004) presented a multi-disciplinary approach to developing organization software for the study of recruitment and group formation. The need to incorporate aspects of social science added a significant contribution to the vision of the resulting Seldon toolkit. The unique addition of an abstract agent category provided a means for capturing social concepts like cliques, gangs, schools, mosque, etc. in a manner that represents their social conceptualization and not simply as a physical or economical institution. This work provides an overview of the Seldon toolkit and terrorist model developed to study the formation of cliques, which are the primary recruitment entity for terrorist organizations. This is a hybrid architecture providing a unique integration of technology and concepts from interdisciplinary fields of agent-based modeling, social science and simulation. This architecture differs from traditional computational social dynamics simulations because of its multi-level design, abstract agent(s), and interaction based on social networks. The supporting social terrorist model is based upon the work of Marc Sageman (2004). Marc Sageman, is a former Foreign Service officer who was based in Islamabad from 1987 to 1989, where he worked closely with Afghanistan’s Mujahedin. Sageman work reveals that the mujahedin have no documented history of psychological or social pathologies; they are considered healthy [members of their society.]	[Abstract] The Seldon project represents a multi-disciplinary approach to developing organization software for the study of recruitment and group formation. The need to incorporate aspects of social science added a significant contribution to the vision of the resulting Seldon toolkit. The unique addition of an abstract agent category provided a means for capturing social concepts like cliques, gangs, schools, mosque, etc. in a manner that represents their social conceptualization and not simply as a physical or economical institution. This paper provides an overview of the Seldon toolkit and terrorist model developed to study the formation of cliques, which are the primary recruitment entity for terrorist organizations. [...] [right column] The general Seldon toolkit is a hybrid architecture providing a unique integration of technology and concepts from the interdisciplinary fields of agent-based modeling, social science, and simulation. This architecture differs from traditional computational social dynamic simulations because of its multi-level design, abstract agent(s), and interactions based on social networks. [...] [page 2, left column] The supporting social terrorist model is based upon the work of Marc Sageman (Sageman 2004). Marc Sageman, Ph.D., M.D., is a former Foreign Service officer who was based in Islamabad from 1987 to 1989, where he worked closely with Afghanistan's mujahedin. [...] Sageman work reveals that the mujahedin have no documented history of psychological or social pathologies: they are considered healthy members of their society.

Farbig

Anmerkungen

The description of the work of Berry et al. is actually taken from parts of their paper. Could also be classified as a pawn sacrifice, a "Bauernopfer". The incorrect grammar from Berry in the last sentence ("Sageman work" instead of "Sageman's work") is incorrect both in Berry *et al* and in Nm.

[97.] Nm/Fragment 085 01

Verschleierung

Untersuchte Arbeit: Seite: 85, Zeilen: 1-7	Quelle: Berry_etal_2004 Seite(n): 2, Zeilen: left column: 15-20
He further states that they have formed into social networks or “clusters” based on some common experience. Their commonality is based on their expatriate status which results in a level of isolation. Their status in the host country and their shared assumed sense of isolation result in the development of clusters. Berry N. *et al* integrated agent based and social modeling approach in the Seldon project.	Second, they have formed into social networks or ‘clusters’ based on some common experience. Their commonality is based on their expatriate status which results in a level of isolation. Their status in their host country and their shared assumed sense of isolation result in the development of clusters. [...] This analysis of the basis for participation supports the integrated agent-based and social network modeling approach we have taken with Seldon.

Farbig

Anmerkungen

The source is only mentioned in the last sentence, the extent of the text taken is not made clear.

[98.] Nm/Fragment 085 08

Verschleierung

Untersuchte Arbeit: Seite: 85, Zeilen: 8-27	Quelle: Clauset_Young_2005 Seite(n): 5, Zeilen: 5: 1st column, 36ff;
In exploring the distribution of the severity of events in global terrorism, Clauset Aaron and Maxwell Young (2005) found a surprising and robust feature: scale invariance. Traditional analyses of terrorism have typically viewed catastrophic events such as the 1995 truck bombing of the American embassy in Nairobi, Kenya, which killed or injured more than 5200. However, the property of scale invariance suggests that these are instead a part of a statistically significant global pattern in terrorism. Further, they showed that there is little reason to believe that the appearance of power laws in the distribution of the severity of an event is the result of either reporting bias or changes in database management. There are many generative mechanisms in the literature for power laws, although many of them are unappealing for explaining the structure (Maxwell Young, 2005) found in global terrorism. The highly abstract model of competition between non-state actors and states, which they proposed, analyzed and extended via the mixtures model, is likely to be too simple to capture the fine structure of global terrorism. However, their model and the statistically significant empirical regularities which showed by the author will frame future efforts to understand global terrorism.	In exploring the distribution of the severity of events in global terrorism, we have found a surprising and robust feature: scale invariance. Traditional analyses of terrorism have typically viewed catastrophic events such as the 1995 truck bombing of the American embassy in Nairobi, Kenya, which killed or injured more than 5 200, as outliers. However, the property of scale invariance suggests that these are instead a part of a statistically significant global pattern in terrorism. Further, we find little reason to believe that the appearance of power laws in the distribution of the severity of an event is the result of either reporting bias or changes in database management. [...] [2nd column, 31ff] There are many generative mechanisms in the literature for power laws, although many of them are unappealing for explaining the structure we find in global terrorism. The highly abstract model of competition between non-state actors and states, which we propose, analyze and extend via the mixtures model, is likely too simple to capture the fine structure of global terrorism. However, we hope that our model and the statistically significant empirical regularities which we show here will frame future efforts to understand global terrorism.

Farbig

Anmerkungen

In describing the findings of Clauset & Young (2005), Nm actually copies quite literally from their paper, which is not mentioned in the bibliography. Note that reference is also made to "Maxwell Young, 2005", which, however, is probably meant to be the same paper. The name of the first author is Aaron Clauset, not Clauset Aaron.

One could also classify this as a pawn sacrifice ("Bauernopfer"), since a partial reference is given, although the extent of the text taken is not make clear.

[99.] Nm/Fragment 085 28

Verschleierung

Untersuchte Arbeit: Seite: 85, Zeilen: 28-32	Quelle: Xu etal 2004 Seite(n): 6, Zeilen: 18ff	Farbig
2.13.2 Statistical Methods	3.1.2 Statistical Methods	
Statistical analysis examines social network dynamics quantitatively. It aims not only to identify and examine the network changes, but also to account for the causes which brought these changes. Structural changes are assumed to result from some [stochastic processes of network effects such as reciprocity, transitivity, and balance (Snijders, T.A.B., 2001).]	Statistical analysis of social network dynamics aims not only at detecting and describing network changes but also at explaining why these changes occur. With statistical methods, structural changes are assumed to result from some stochastic processes of network effects such as reciprocity, transitivity, and balance [EN 34].	
	[EN 34]. Snijders, T.A.B. (2001). The statistical evaluation of social network dynamics. *Sociological Methodology*, 31, 361-395.	

Anmerkungen

No source given. Text continues on the next page: Nm/Fragment_086_01

[100.] Nm/Fragment 086 01

Verschleierung

Untersuchte Arbeit: Seite: 86, Zeilen: 1-15	Quelle: Xu etal 2004 Seite(n): 6-7, Zeilen: 6: 20ff; 7: 1ff	Farbig
[Structural changes are assumed to result from some] stochastic processes of network effects such as reciprocity, transitivity, and balance (Snijders, T.A.B., 2001). In statistical analysis, links are modeled as random variables that can be in different states at different times. The purpose is to identify which network models fits best with empirical data and observed structural changes.	With statistical methods, structural changes are assumed to result from some stochastic processes of network effects such as reciprocity, transitivity, and balance [EN 34]. In this type of analysis, links are modeled as random variables that can be in different states [...] at different time. The [P. 7] purpose is to examine which network effect fits the empirical data and better accounts for the observed structural changes.	
Discrete or continuous Markov models are often used in statistical analysis. The Markov models are based on the assumptions that a particular state of a process is dependent current state but not on any previous state (Leenders, R., 1997; Snijders, T.A.B., 1997; Snijders, T.A.B., 2001). The analysis is carried out with the help of transition and intensity matrix. Transition matrix contains the conditional probabilities one state to previous state, while the intensity matrix contains the transition rates (Hallinan, M.T.,1978/79); Leenders, R., 1997).	Discrete or continuous Markov models are often used in statistical analysis. The most important property of a Markov model is that the future state of a process is dependent only on the current state but not on any previous state [EN 25, EN 33, EN 34]. The process is governed by a transition matrix, which contains the conditional probabilities of changing from the initial state to the current state, and the intensity matrix whose elements are transition rates [EN 19, EN 25].	
	[EN 19] Hallinan, M.T. (1978/79). The process of friendship formation. *Social Networks*, 1, 193-210. [EN 25] Leenders, R. (1997). Evolution of friendship and best friendship choices, in *Evolution of social networks*, P. Doreian & F.N. Stokman (eds.). Gordon and Breach: Australia. [EN 33] Snijders, T.A.B. (1997). Stochastic actor-oriented models for network change, in *Evolution of social networks*, P. Doreian & F.N. Stokman (eds.). Gordon and Breach: Australia. [EN 34] Snijders, T.A.B. (2001). The statistical evaluation of social network dynamics. *Sociological Methodology*, 31, 361-395.	

Anmerkungen

Copied text starts on the previous page (Nm/Fragment_085_28). No source is given.

[101.] Nm/Fragment 086 25

Verschleierung

Untersuchte Arbeit: Seite: 86, Zeilen: 25-32	Quelle: Xu etal 2004 Seite(n): 7, Zeilen: 16ff	Farbig
2.13.3 Simulation Methods	*3.1.3 Simulation Methods*	
The simulation methods exploit multi agent technology to analyse the network dynamics, in contrary to descriptive or statistical methods which examine social network dynamics quantitatively. In the simulation method, members in a social network are often modeled intelligent agents with ability to behave and make decisions based on certain criteria in a particular situation. The collective behaviors of all members in a network will determine [how the network evolves from one structure to another in a considered scenario.]	Unlike descriptive or statistical methods, which examine social network dynamics quantitatively, simulation methods rely on multi-agent technology to analyze network dynamics. In this method, members in a social network are often modeled and implemented as computer agents who have the abilities to behave and make decisions based on certain criteria. The collective behaviors of all members in a network will determine how the network evolves from one structure to another.	

Anmerkungen

No source given.

[102.] Nm/Fragment 087 01

Verschleierung

Untersuchte Arbeit: Seite: 87, Zeilen: 1-11	Quelle: Xu etal 2004 Seite(n): 7, 8, Zeilen: 7: 20ff; 8: 1ff	Farbig
[The collective behaviors of all members in a network will determine] how the network evolves from one structure to another in a considered scenario.	The collective behaviors of all members in a network will determine how the network evolves from one structure to another.	
There are many examples of employing simulation methods in social network analysis. For instance, Ornstein employs agent-based simulation to identify how social choices of establishing or ceasing a relationship with others affect the overall structure of a network (Hummon, N.P., 2000). The basic assumption is that every relationship has an associated costs and benefits. Individuals aim to maximize their utilities by altering their relationships with others and social network will keep on evolving until joint utility of all members is maximized.	Several SNA studies have employed simulation methods. For example, Ornstein uses agent-based simulation to study how individuals' social choices of establishing or ceasing a [P. 8] relationship with others affect the structure of a network [EN 20]. The basic assumption is that maintaining a relationship has its associated costs and benefits and individuals aim to maximize their utilities by altering their relationships with others. A social network will keep changing until the joint utility of all members is maximized. --- [EN 20] Hummon, N.P. (2000). Utility and dynamic social networks. *Social Networks*, 22, 221-249.	

Anmerkungen

No source given

[103.] Nm/Fragment 087 12

Verschleierung

Untersuchte Arbeit: Seite: 87, Zeilen: 12-32	Quelle: CNS_2002 Seite(n): 18, 105, Zeilen: 18:16-17; 105:14ff

Farbig

Professor Carley and her colleagues are working on a number of projects related to counterterrorism. All their models contain AI, complexity approaches, and are multi-agent.

- BIOWAR –Carley, K., M.; Douglas B. Fridsma; Alex Yahja (2002) described “BIOWAR”; a simulation system that uses cognitively realistic agents embedded in social, knowledge and work networks. The idea is to describe how people participating in these networks acquire disease, manifest symptoms, seek information and treatment, and recover from illness. The system uses a model of diseases and symptoms to analyse the agents who come in contact with infectious agents through their social and work networks become ill. The illnesses alter their behavior, changing both the propagation of the disease, and the manifestation of the disease on the population. A number of simulations were completed by them that were targeted to examine the effect of contagious and non-contagious illnesses in high-alert (agents have knowledge of a potential disease outbreak) or low alert states. Agents who believe they may be ill and have knowledge of a potential outbreak are more likely to seek care than those who do not.

Professor Carley described six ongoing projects related to counterterrorism being conducted by her research group. All their models contain AI, complexity approaches, and are multi-agent.

[page 105]

We describe a simulation system called BIOWAR which uses cognitively realistic agents embedded in social, knowledge and work networks to describe how people interacting in these networks acquire disease, manifest symptoms, seek information and treatment, and recover from illness. Using a model of diseases and symptoms, agents who come in contact with infectious agents through their social and work networks become ill. These illnesses alter their behavior, changing both the propagation of the disease, and the manifestation of the disease on the population.

Presently, we have completed a number of simulations which examine the effect of contagious and non-contagious illnesses in high-alert (agents have knowledge of a potential disease outbreak) or low alert states. Agents who believe they may be ill and have knowledge of a potential outbreak are more likely to seek care than those who do not.

Anmerkungen

No source given

[104.] Nm/Fragment 088 01

Verschleierung

Untersuchte Arbeit: Seite: 88, Zeilen: 1-20	Quelle: CNS_2002 Seite(n): 18, 105, Zeilen: 105:23-29; 18:18-21;23-24

Farbig

[In this] system authors compared results of low alert states to known influenza epidemics and to data containing emergency room visits, pharmacy purchases and absenteeism. Although the peak incidence of the simulated outbreak is larger than the peak incidence seen in the population data, the simulation results are temporally similar to those seen in the population data. They hoped that this simulation framework will allow them to ask ‘what-if’ questions regarding appropriate response and detection strategies for both natural and man-made epidemics. This is a city scale multi-agent model of weaponized bioterrorist attacks for intelligence and training. At present the model is running with 100,000 agents (this number will be increased). All agents have real social networks and the model contains real city data -hospitals, schools etc. Agents are as realistic as possible and contain a cognitive model.

- DYNET—Dynamic Networks. The team is building a model of how networks adapt, evolve and change in response to various types of attacks e.g. infowar or assassination.

[page 105]

We have compared results of low alert states to known influenza epidemics and to data containing emergency room visits, pharmacy purchases and absenteeism. Although the peak incidence of the simulated outbreak is larger than the peak incidence seen in the population data, the simulation results are temporally similar to those seen in the population data. [...]. It is hoped that this simulation framework will allow us to ask ‘what-if’ questions regarding appropriate response and detection strategies for both natural and man-made epidemics.

[page 18]

this is a cityscale multi-agent model of weaponized bioterrorist attacks for intelligence and training. At present the model is running with 100,000 agents (this number will be increased). All agents have real social networks and the model contains real city data - hospitals, schools etc. Agents are as realistic as possible and contain a cognitive model.

[...]

DYNET – Dynamic Networks. The team is building a model of how networks adapt, evolve and change in response to various types of attacks e.g. infowar or assassination

Anmerkungen

No source given

[105.] Nm/Fragment 088 21

Verschleierung

Untersuchte Arbeit: Seite: 88, Zeilen: 21-33	Quelle: Dombroski Carley 2002 Seite(n): 1, Zeilen: 14-24	Farbig
NETEST – It is based on the combination of multi-agent technology with hierarchical Bayesian inference models and biased net models to produce accurate posterior network representations. Bayesian inference models produce representations of a network's structure and informant accuracy by combining prior network and accuracy data with informant perceptions of a network. Biased net theory examines and captures the biases that may be present within a specific network or group of networks. NETEST provides functionalities to estimate a network's size, determine its membership and structure, determine areas of the network where data is missing, perform cost and benefit analysis of additional information, assess group level capabilities [embedded in the network, and pose "what if" scenarios to destabilize a network and predict its evolution over time.]	NETEST is a tool that combines multiagent technology with hierarchical Bayesian inference models and biased net models to produce accurate posterior representations of a network. Bayesian inference models produce representations of a network's structure and informant accuracy by combining prior network and accuracy data with informant perceptions of a network. Biased net theory examines and captures the biases that may exist in a specific network or set of networks. Using NETEST, an investigator has the power to estimate a network's size, determine its membership and structure, determine areas of the network where data is missing, perform cost/benefit analysis of additional information, assess group level capabilities embedded in the network, and pose "what if" scenarios to destabilize a network and predict its evolution over time.	

Anmerkungen

The source is given in the bibliography, but nowhere close to this text fragment.

[106.] Nm/Fragment 089 01

Verschleierung

Untersuchte Arbeit: Seite: 89, Zeilen: 1-2	Quelle: Dombroski Carley 2002 Seite(n): 1, Zeilen: 20-24	Farbig
[NETEST provides functionalities to estimate a network's size, determine its membership and structure, determine areas of the network where data is missing, perform cost and benefit analysis of additional information, assess group level capabilities] embedded in the network, and pose "what if" scenarios to destabilize a network and predict its evolution over time.	Using NETEST, an investigator has the power to estimate a network's size, determine its membership and structure, determine areas of the network where data is missing, perform cost/benefit analysis of additional information, assess group level capabilities embedded in the network, and pose "what if" scenarios to destabilize a network and predict its evolution over time.	

Anmerkungen

The copied text starts on the previous page. A reference is not given.

[107.] Nm/Fragment 089 03

Verschleierung

Untersuchte Arbeit: Seite: 89, Zeilen: 3-25	Quelle: CNS_2002 Seite(n): 14, 18, 20, Zeilen: 14: 11-17; 18: 28-31; 20: 23-26
THREATFINDER – this tool originated in the corporate realm. Certain individuals within an organization are more likely than others to pose threats. The research involves looking for threat indicators for who could launch an attack i.e. using a network/organizational perspective, Threatfinder identifies threats within an organization. Tsvetovat Maksim and Kathleen Carley (2002) proposed a methodology for realistically simulating terrorist networks in order to develop network metrics to test strategies of destabilizing them, provided a model of antiterrorist policy. They have not discussed behavior or real group interaction and the model is limited in scope and depth. It may be used as a starting point to focus terrorist organization and network Michael J. North and his colleagues (North, J. M; Nicholson, T. C; and Jerry R. V., 2006) worked on a model of terrorist networks— looking at relationships between different terrorist structures. Their models show whether or not particular terrorist group fits in a given structure. The authors modeled terrorists as genetic algorithms. The models also look at counter forces. Social factors, such as propagation of dangerous ideas, are built into the model. The model uses REPAST tool (developed by University of Chicago) which, as opposed to SWARM (which they believe is getting old).	[page 18] THREATFINDER – this tool originated in the corporate realm. Certain individuals within an organization are more likely than others to pose threats. The research involves looking for threat indicators for who could launch an attack i.e. using a network/organizational perspective, Threatfinder identifies threats within an organization. [page 20] The paper proposes a methodology for realistically simulating terrorist networks in order to develop network metrics to test strategies of destabilizing them; provides a model of anti-terrorist policy; doesn't provide behavior or real group interaction and is limited in scope and depth; may be used as a starting point; focus: terrorist organization and network [page 14] - He is working on a model of terrorist networks – looking at relationships between different terrorist structures. - His models let people test whether or not a particular terrorist group fits a given structure. - Terrorists are modeled as genetic algorithms. - The model also looks at counterforces. - Social factors, such as the propagation of dangerous ideas, are built into the model. - The model uses REPAST (developed by the University of Chicago) which is written in Java, as opposed to SWARM which is written in C (and he believes is getting old).

Farbig

Anmerkungen

No source given

[108.] Nm/Fragment 090 13

KomplettPlagiat

Untersuchte Arbeit: Seite: 90, Zeilen: 13-24	Quelle: Xu etal 2004 Seite(n): 8, 10, Zeilen: 8: 11ff; 10: 4ff
Some SNA research, especially citation analysis, has employed visualization techniques to study network dynamics. This approach relies on visual presentations of social networks and is quite different from descriptive, statistical, and simulation methods. **2.14 SUMMARY** The research in the dynamic of SNA studies provides a good foundation for criminal network dynamics analysis. Although the purpose of analyzing criminal network dynamics is not to test theories, the methods, measures, and models from SNA can help detect and describe structural changes, extract the patterns of these changes, and even predict the future activities and structure of criminal organizations.	Some SNA research, especially citation analysis, has employed visualization techniques to study network dynamics. This approach relies on visual presentations of social networks and is quite different from the descriptive, statistical, and simulation methods. [...] [Page 10] Research in these dynamic SNA studies provides a good foundation for criminal network dynamics analysis. Although the purpose of analyzing criminal network dynamics is not to test theories, the methods, measures, and models from SNA can help detect and describe structural changes, extract the patterns of these changes, and even predict the future activities and structure of criminal organizations.

Farbig

Anmerkungen

Word-by-word copy from the source. The source is not referenced.

[109.] Nm/Fragment 091 11

Verschleierung

Untersuchte Arbeit: Seite: 91, Zeilen: 11-20	Quelle: Ressler 2006 Seite(n): 4, Zeilen: 8-13
Moreover, as described earlier, data collection is difficult for any network analysis because it is hard to create a complete network. It is difficult especially to gain information on terrorist networks. Terrorist organizations do not provide information on their membership structure, and the intelligence agencies rarely allow researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through descriptive and straight forward methods (for example, Krebs V., 2002, Sageman, M., 2004) as described earlier.	Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling.

Farbig

Anmerkungen

Unbelievable: For the third time (see Nm/Fragment_033_15 and Nm/Fragment_040_22) we are confronted with the same six lines from Ressler (2006) with only slight modifications. Still no mention of the source.

[110.] Nm/Fragment 091 21

Verschleierung

Untersuchte Arbeit: Seite: 91, Zeilen: 21-28	Quelle: Ressler 2006 Seite(n): 4, 5, Zeilen: p.4,44-46 - p.5,1-3
One promising activity is the development of a major terrorism web portal at the University of Arizona's Artificial Intelligence Lab. The website makes social network tools and data related to terrorism publicly available (Reid, E., *et al*., 2004). One example is the Terrorism Knowledge Portal, a database consisting of over 360,000 terrorism news articles and related Web pages coming from various high-quality terrorism websites, major search engines, and new portals.	[p. 6] One promising activity is the development of a major terrorism web portal at the University of Arizona's Artificial Intelligence Center. This website makes social network tools and data related to terrorism publicly available. [EN 18] One example is the Terrorism [p.7] Knowledge Portal, a database consisting of over 360,000 terrorism news articles and related Web pages coming from various high-quality terrorism Web sites, major search engines, and news portals. [EN 18] Edna Reid, Jialun Quin, Wingyan Chung, Jennifer Xu, Yilu Zhou, Rob Schumaker, Marc Sageman, and Hsinchun Chen, "Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Address the Threats of Terrorism," (Working paper, 2004).

Farbig

Anmerkungen

Nothing marked as a citation, no source named.

[111.] Nm/Fragment 093 04

Verschleierung

Untersuchte Arbeit: Seite: 93, Zeilen: 4-16	Quelle: Xu_and_Chen_2003 Seite(n): 232, Zeilen: 22ff	Farbig
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 for the basis of terrorism 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, groups or cells, within which members have close relationships, may be present. 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. Some 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, [...] 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 [...]. 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.	

Anmerkungen

"Criminals" become "Terrorists", and a few more adaptations. The original source is not referenced.

Note that the very same paragraph can also be found at the beginning of the thesis: Nm/Fragment_019_01

[112.] Nm/Fragment 093 17

Verschleierung

Untersuchte Arbeit: Seite: 93, Zeilen: 17-25	Quelle: Katz et al 2004 Seite(n): 308, Zeilen: 23-31	Farbig
In social network literature, researchers have examined a broad range of types of ties (Menzel, H. and Katz, E., 1957). 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.	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.	

Anmerkungen

The source of this section is found in the list of references but not here. Moreover nothing is marked as a citation.

Note: Page 19 and page 93 of the thesis are nearly identical, so Katz et al. (2004) has also been copied on page 19: Nm/Fragment_019_16

[113.] Nm/Fragment 094 01

Verschleierung

Untersuchte Arbeit: Seite: 94, Zeilen: 1-25	Quelle: Katz et al 2004 Seite(n): 308-309, Zeilen: p.308,31-33 - p.309,1-11.13-20
For example, two terrorists might have a formal tie (one is a footsoldier or a newly recruited person in a terrorist cell and reports to another, who is a cell leader) and an affective tie (they are friends); and may also have a proximity tie (i.e., they reside in the same building and their apartments are two doors away on the same floor). Network researchers have distinguished between strong ties (such as family and friends) and weak ties such as acquaintances (Granovetter, M., 1973, 1982). 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. Ties may be non-directional (for example, Atta attends 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 Khalid about 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).	[p. 308] 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) [p.309] and an affective tie (they are friends) and a proximity tie (their offices are two doors away). 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. [...] 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).

Farbig

Anmerkungen

The same text, only the examples have been adapted to the subject at hand, terrorism. No reference given.

[114.] Nm/Fragment 094 28

Verschleierung

Untersuchte Arbeit: Seite: 94, Zeilen: 28-32	Quelle: Xu and Chen 2003 Seite(n): 232, Zeilen: 32-36
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.]	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.

Farbig

Anmerkungen

nothing marked as a citation, no reference given

[115.] Nm/Fragment 095 01

Verschleierung

Untersuchte Arbeit: Seite: 95, Zeilen: 1-8	Quelle: Xu and Chen 2003 Seite(n): 233, Zeilen: 1-4	Farbig
For example, capture of central members in a network may effectively upset the operational network and put a terrorist organization out of action (Baker, W.E. and Faulkner, R.R., 1993; McAndrew, D., 1999; Sparrow, M., 1991). Subgroups and interaction patterns between groups are helpful in finding a network's overall structure, which often reveals points of vulnerability (Evan, W. M., 1972; Ronfeldt, D., Arquilla, J., 2001).	[For exam]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].	

[EN 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.

[EN 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.

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

[EN 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.

[EN 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).

Anmerkungen

Continuation from previous page.

This section appears in Nm's thesis for the second time, the first time was here: Nm/Fragment 021 01

[116.] Nm/Fragment 095 12

KomplettPlagiat

Untersuchte Arbeit: Seite: 95, Zeilen: 12-15	Quelle: Borgatti_2002 Seite(n): 1, Zeilen: 8-10	Farbig
Graph Theory [FN 14] The fundamental concept of graph theory is a graph, which (despite the name) is best thought of as a mathematical object rather than a diagram, even though graphs have a very natural graphical representation.	**Graphs** The fundamental concept of graph theory is the graph, which (despite the name) is best thought of as a mathematical object rather than a diagram, even though graphs have a very natural graphical representation.	

[FN 14] Most of the concepts discussed in this section are taken from West B. Douglas (2001).

Anmerkungen

The source is not given. West B. Douglas is listed in the bibliography under "West", but the author is named Douglas B. West and the book was published in 1996 (2nd edition was 2001): http://www.math.uiuc.edu/~west/igt/

[117.] Nm/Fragment 096 02

Verschleierung

Untersuchte Arbeit: **Seite: 96, Zeilen: 2-20**	**Quelle: Borgatti_2002** **Seite(n): 2, Zeilen: 1ff** Farbig
When looking at visualizations of graphs such as Figure 3.1, it is important to realize that the only information contained in a diagram is adjacency; the position of nodes in a plane (and therefore the length of lines) is arbitrary unless otherwise specified. Hence it is usually dangerous to draw conclusions based on the spatial position of the nodes. For example, it is tempting to conclude that nodes in the middle of a diagram are more important than nodes on the peripheries, but this will often – if not usually – be a mistake.	When looking at visualizations of graphs such as Figure 1, it is important to realize that the only information contained in the diagram is adjacency; the position of nodes in the plane (and therefore the length of lines) is arbitrary unless otherwise specified. Hence it is usually dangerous to draw conclusions based on the spatial position of the nodes. For example, it is tempting to conclude that nodes in the middle of a diagram are more important than nodes on the peripheries, but this will often – if not usually – be a mistake.
When using graphs to represent terrorist networks, we typically use each line to represent instances of the same social relation, so that if (a, b) indicates a friendship between a person located at node a, and a person located at node b, then (d, e) indicates a friendship between d and e. Thus, each distinct social relation that is empirically measured on the same group of people is represented by separate graphs, which are likely to have different structures (after all, who talks to whom, is not the same as who dislikes whom).	When used to represent social networks, we typically use each line to represent instances of the same social relation, so that if (a, b) indicates a friendship between the person located at node a and the person located at node b, then (d, e) indicates a friendship between d and e. Thus, each distinct social relation that is empirically measured on the same group of people is represented by separate graphs, which are likely to have different structures (after all, who talks to whom is not the same as who dislikes whom).
The natural graphical representation of an adjacency matrix is a [table, such as shown in Figure 3. 2.]	[...] The natural graphical representation of an adjacency matrix is a table, such as shown in Figure 2.

Anmerkungen

The source is not given. Note the slight adaptation to make the text fit the terrorist topic of the thesis.

[118.] Nm/Fragment 097 01

Verschleierung

Untersuchte Arbeit: **Seite: 97, Zeilen: 1-8**	**Quelle: Borgatti_2002** **Seite(n): 2, Zeilen: 15ff** Farbig
[The natural graphical representation of an adjacency matrix is a] table, such as shown in Figure 3. 2.	The natural graphical representation of an adjacency matrix is a table, such as
[TABLE, same as in source but extended by one row and one column]	shown in Figure 2.
Figure 3.2. Adjacency matrix for graph in Figure 3.1.	[TABLE]
Examining either Figure 3.1 or Figure 3.2, we can see that not every vertex is adjacent to every other. A graph in which all vertices are adjacent to all others is said to be complete. The extent to which a graph is complete is indicated by its density, which is defined as the number of edges divided by the number possible. If self-loops are excluded, then the number possible is n(n-1)/2. Hence the density of the graph in Figure 3.1 is 7/21 = 0.33.	Figure 2. Adjacency matrix for graph in Figure 1. Examining either Figure 1 or Figure 2, we can see that not every vertex is adjacent to every other. A graph in which all vertices are adjacent to all others is said to be complete. The extent to which a graph is complete is indicated by its density, which is defined as the number of edges divided by the number possible. If self-loops are excluded, then the number possible is n(n-1)/2. [...] Hence the density of the graph in Figure 1 is 6/15 = 0.40.

Anmerkungen

The source is not given anywhere in the thesis.

[119.] Nm/Fragment 097 09

Verschleierung

Untersuchte Arbeit: Seite: 97, Zeilen: 9-19	Quelle: Brandes_Erlebach_2005 Seite(n): 7, 8, Zeilen: p7: 30ff; p8: 1ff
Graphs can be *undirected* or *directed*. The adjacency matrix of an undirected graph (as shown in Figure 3.2) is symmetric. An undirected edge joining vertices $u, v \in V$ is denoted by $\{u, v\}$. In *directed* graphs, each directed edge (arc) has an *origin* (*tail*) and a *destination* (*head*). An edge with origin $u \in V$ is represented by an order pair (u, v). As a shorthand notation, an edge $\{u, v\}$ can also be denoted by uv. It is to note that, in a *directed* graph, uv is short for (u, v), while in an *undirected* graph, uv and vu are the same and both stands for $\{u, v\}$. Graphs that can have directed as well undirected edges are called *mixed graphs*, but such graphs are encountered rarely.	Graphs can be *undirected* or *directed*. In undirected graphs, the order of the endvertices of an edge is immaterial. An undirected edge joining vertices $u, v \in V$ is denoted by $\{u, v\}$. In directed graphs, each directed edge (arc) has an *origin* (*tail*) and a *destination* (*head*). An edge with origin $u \in V$ and destination $v \in V$ is represented by an ordered pair (u, v). As a shorthand notation, an edge $\{u, v\}$ or (u, v) can also be denoted by uv. In a directed graph, uv is short for (u, v), while in an undirected graph, uv and vu are the same and both stand for $\{u, v\}$. [...]. Graphs that can have directed edges as well as undirected edges are called *mixed graphs*, but such graphs are encountered rarely [...]

Farbig

Anmerkungen

The source is not mentioned anywhere in the thesis.

The definitions given here are certainly standard and don't need to be quoted. However, Nm uses for several passages the same wording as the source.

Note also that "An edge with origin $u \in V$ is represented by an order pair (u, v)" is a curious abbreviation of the statement "An edge with origin $u \in V$ and destination $v \in V$ is represented by an ordered pair (u, v)" in the source.

[120.] Nm/Fragment 098 09

KomplettPlagiat

Untersuchte Arbeit: Seite: 98, Zeilen: 9-22	Quelle: Borgatti_2002 Seite(n): 3, Zeilen: 1ff
Similarly, any pair of vertices in which one vertex can reach the other via a sequence of adjacent vertices is called *reachable*. If we determine reachability for every pair of vertices, we can construct a reachability matrix R such as depicted in Figure 3.3. The matrix R can be thought of as the result of applying transitive closure to the adjacency matrix A. [FIGURE, different from source] **Figure 3.3. Reachability matrix** A *component* of a graph is defined as a maximal subgraph in which a path exists from every node to every other (i.e., they are mutually reachable). The size of a component is defined as the number of nodes it contains. A connected graph has only one component. A sequence of adjacent vertices $v_0, v_1, \ldots, v_n$ is known as a *walk*. A walk can also be seen as a sequence of *incident* edges, where two edges are said to be incident if they share exactly one vertex. A walk in which no vertex occurs more than once is known as a *path*.	Similarly, any pair of vertices in which one vertex can reach the other via a sequence of adjacent vertices is called reachable. If we determine reachability for every pair of vertices, we can construct a reachability matrix R such as depicted in Figure 3. The matrix R can be thought of as the result of applying transitive closure to the adjacency matrix A. [FIGURE] **Figure 3** A *component* of a graph is defined as a maximal subgraph in which a path exists from every node to every other (i.e., they are mutually reachable). The size of a component is defined as the number of nodes it contains. A connected graph has only one component. A sequence of adjacent vertices $v_0, v_1, \ldots, v_n$ is known as a *walk*. [...]. A walk can also be seen as a sequence of *incident edges*, where two edges are said to be incident if they share exactly one vertex. A walk in which no vertex occurs more than once is known as a *path*.

Farbig

Anmerkungen

No source given. The table Nm gives (figure 3.3.) can be found in the source on page 4 (figure 4).

[121.] Nm/Fragment 099 01

Verschleierung

Untersuchte Arbeit: Seite: 99, Zeilen: 1-25	Quelle: Borgatti_2002 Seite(n): 3-4, Zeilen: p3: 13ff; p4: 1ff
A walk in which no edge occurs more than once is known as a *trail*. In Figure 3.1, the sequence a, b, c, e, d, c, g is a trail but not a path. Every path is a trail, and every trail is a walk. A walk is closed if $v_o = v_n$. A *cycle* can be defined as a closed path in which n >= 3. The sequence c, e, d in Figure 3.1 is a cycle. A *tree* is a connected graph that contains no cycles. In a tree, every pair of points is connected by a unique path. That is, a tree is a graph in which any two vertices are connected by *exactly one* path.	A walk in which no edge occurs more than once is known as a *trail*. In Figure 3, the sequence a, b, c, e, d, c, g is a trail but not a path. Every path is a trail, and every trail is a walk. A walk is closed if $v_o = v_n$. A cycle can be defined as a closed path in which n >= 3. The sequence c, e, d in Figure 3 is a cycle. A *tree* is a connected graph that contains no cycles. In a tree, every pair of points is connected by a unique path. That is, there is only one way to get from A to B.
The length of a walk (and therefore a path or trail) is defined as the number of edges it contains. For example, in Figure 3.1, the path a, b, c, d, e has length 4. A walk between two vertices whose length is as short as any other walk connecting the same pair of vertices is called a *geodesic*. Of course, all geodesics are paths. Geodesics are not necessarily unique. From vertex a to vertex f in Figure 3.1, there are two geodesics: a, b, c, d, e, f and a, b, c, g, e, f.	The length of a walk (and therefore a path or trail) is defined as the number of edges it contains. For example, in Figure 3, the path a, b, c, d, e has length 4. A walk between twovertices whose length is as short as any other walk connecting the same pair of vertices iscalled a *geodesic*. Of course, all geodesics are paths. Geodesics are not necessarily unique. From vertex a to vertex f in Figure 1, there are two geodesics: a, b, c, d, e, f and a, b, c, g, e, f.
The *graph-theoretic distance* (usually shortened to just “distance”) between two vertices is defined as the length of a geodesic that connects them. If we compute the distance between every pair of vertices, we can construct a distance matrix D such as depicted in Figure 3.3. The maximum distance in a graph defines the graph’s diameter. As shown in Figure 3.3, the diameter of the graph in Figure 3.1 is 4. If the graph is not connected, then there exist pairs of vertices that are not mutually reachable so that the distance between them is not defined and the diameter of such a graph is also not defined.	The *graph-theoretic distance* (usually shortened to just “distance”) between two vertices is defined as the length of a geodesic that connects them. If we compute the distance between every pair of vertices, we can construct a distance matrix D such as depicted in Figure 4. The maximum distance in a graph defines the graph’s diameter. As shown in [page 4] Figure 4, the diameter of the graph in Figure 1 is 4. If the graph is not connected, then there exist pairs of vertices that are not mutually reachable so that the distance between them is not defined and the diameter of such a graph is also not defined.

Farbig

Anmerkungen

No source given, very minor adjustments

[122.] Nm/Fragment 099 26

KomplettPlagiat

Untersuchte Arbeit: Seite: 99, Zeilen: 26-32	Quelle: Brandes_Erlebach_2005 Seite(n): 8, Zeilen: 8-14
In both *undirected* and *directed graphs', we may allow the edge set E to contain the same edge several times, that is,* E *can be a multiset. If an edge occurs several times in* E*, the copies of that edge are called* parallel edges*. Graphs with parallel edges are also called* multigraphs*. A graph is called* simple*, if each of its edges is contained in* E *only once, i.e., if the graph does not have parallel edges. An edge joining a vertex to itself, i.e., and edge whose end [vertices are identical, is called a* loop*.]*	In both undirected and directed graphs, we may allow the edge set *E* to contain the same edge several times, i.e., *E* can be a multiset. If an edge occurs several times in *E*, the copies of that edge are called *parallel edges*. Graphs with parallel edges are also called *multigraphs*. A graph is called *simple*, if each of its edges is contained in *E* only once, i.e., if the graph does not have parallel edges. An edge joining a vertex to itself, i.e., an edge whose endvertices are identical, is called a *loop*.

Farbig

Anmerkungen

The source is not given.

The definitions given here are certainly standard and don't need to be referenced. Nm, however, copied the formulation of those definitions word for word.

[123.] Nm/Fragment 100 01

Verschleierung

Untersuchte Arbeit:
Seite: 100, Zeilen: 1-16

A graph is called loop-free if it has no loops.

A graph $G' = (V', E')$ is a subgraph of the graph $G = (V, E)$ if $V' \subset V$ and $E' \subset E$. It is a (vertex-)induced graph if E' contains all edges $e \in E$ that join vertices in V'.

Often it is useful to associate numerical values (weights) with the edges or vertices of a graph $G = (V, E)$. The graph having weights is known as *weighted graph*. Here we only discuss edge weights. Edge weights can be represented as a function $\omega : E \to \mathbb{R}$ that assigns each edge $e \in E$, a weight $\omega(e)$. Depending on the context, edge weights can describe various properties such as strength of interaction, or similarity. One usually tries to indicate the characteristics of the edge weights by the choice of the name of the function. For most purposes, an unweighted graph $G = (V, E)$ is equivalent to a weighted graph with unit edge weights $\omega(e) = 1$ for all $e \in E$.

Quelle: Brandes_Erlebach_2005
Seite(n): 8, 9, Zeilen: -

Farbig

[Page 8, line 14]

A graph is called loop-free if it has no loops.

[Page 9, line 4-6]

A graph $G' = (V', E')$ is a *subgraph* of the graph $G = (V, E)$ if $V' \subset V$ and $E' \subset E$. It is a (vertex-)induced subgraph if E' contains all edges $e \in E$ that join vertices in V'.

[Page 8, line 16ff]

Weighted graphs. Often it is useful to associate numerical values (weights) with the edges or vertices of a graph $G = (V, E)$. Here we discuss only edge weights. Edge weights can be represented as a function $\omega : E \to \mathbb{R}$ that assigns each edge $e \in E$ a weight $\omega(e)$.

Depending on the context, edge weights can describe various properties such as [...] strength of interaction, or similarity. One usually tries to indicate the characteristics of the edge weights by the choice of the name for the function. [...] For most purposes, an unweighted graph $G = (V, E)$ is equivalent to a weighted graph with *unit edge* weights $\omega(e) = 1$ for all $e \in E$.

Anmerkungen

The source is not given.

The definitions given here are certainly standard and don't need to be referenced. The author however copies not only the definitions but also their formulation word for word. The symbol for the real numbers used as the domain of the weight function is reproduced only as a box in the thesis, indicating that this character was not available in the font used.

[124.] Nm/Fragment 100 24

Verschleierung

Untersuchte Arbeit:
Seite: 100, Zeilen: 24-30

A review of key centrality concepts can be found in the papers by Freeman (1978, 1979). This work has contributed significantly 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.

Quelle: Stephenson and Zelen 1989
Seite(n): 2-3, Zeilen: p.2, 31-35 - p.3, 1-3

Farbig

[page 2]

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.

Anmerkungen

Shortened but otherwise identical. Not marked as a citation, no reference given.

[125.] Nm/Fragment 101 01

Verschleierung

Untersuchte Arbeit: Seite: 101, Zeilen: 1-8	Quelle: Scott_1987 Seite(n): 23, Zeilen: 24-28
A central node was one which was at the center of a number of connections, a node with many direct contacts with other nodes. The simplest and most straight-forward way to measure node centrality, therefore, is by the degrees of various nodes in the graph. The degree, is simply the number of other points to which a node is adjacent. A node is central, then, if it has high degree; the corresponding agent is central in the sense of being well connected or in the thick of things.	A central point was one which was 'at the centre' of a number of connections, a point with a great many direct contacts with other points. The simplest and most straightforward way to measure point centrality, therefore, is by the degrees of the various points in the graph. Tle degree, it will be recalled, is simply the number of other points to which a point is adjacent. A point is central, then, if it has a high degree; the corresponding agent is central in the sense of being 'well-connected' or 'in the thick of things'.

Farbig

Anmerkungen

The source is not given here.

[126.] Nm/Fragment 101 20

KomplettPlagiat

Untersuchte Arbeit: Seite: 101, Zeilen: 20-26	Quelle: Koschuetzki_etal_2005 Seite(n): 20, Zeilen: 12-16
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 neighbours.	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.

Farbig

Anmerkungen

The source is not mentioned anywhere in the thesis.

Note, that this paragraph can also be found in other publications of Nm: Memon, Larsen, Hicks & Harkiolakis (2008) (http://books.google.es/books?id=s_OgimTsGtcC&pg=PA479&lpg=PA479&dq=%22represent+a+static+situation+and+we+are+interested+in+the%22&source=bl&ots=0bA-of9GAw&sig=jYUZ9NhqErpmXxp54i9vXsrJVCM&hl=en&sa=X&ei=PWiWT9HTFYnChAf9n8CADg&redir_esc=y#v=onepage&q=%22represent%20a%20static%20situation%20and%20we%20are%20interested%20in%20the%22&f=false) and Memon, Hicks & Larsen (2007) (http://books.google.es/books?id=7URT9Xpfsj4C&pg=PA436&lpg=PA436&dq=%22represent+a+static+situation+and+we+are+interested+in+the%22&source=bl&ots=ejqpQm4Jm9&sig=lJ8pXffJ8C5Nd_eHTz3CiZ3WYic&hl=en&sa=X&ei=PWiWT9HTFYnChAf9n8CADg&redir_esc=y#v=onepage&q=%22represent%20a%20static%20situation%20and%20we%20are%20interested%20in%20the%22&f=false) . Henrik Legind Larsen is the thesis supervisor and David L. Hicks is the thesis committee chairman.

[127.] Nm/Fragment 102 02

Verschleierung

Untersuchte Arbeit: Seite: 102, Zeilen: 2-28	Quelle: Scott_1987 Seite(n): 83-85, Zeilen: p. 83: 33-

Farbig

A degree based measure of node centrality can be extended beyond direct connections to those at various path distances. In this case, the relevant neighbourhood is widened to include the more distant connections of the nodes. A node may, then, be assessed for its local centrality in terms of both direct (distance 1) and distance 2 connections—or, indeed, whatever cut-off path distance is chosen. The principal problem with extending this measure of node centrality beyond distance 2 connections is that, in graphs with even a very modest density, the majority of the nodes tend to be linked through indirect connections at relatively short path distances.

Thus a comparison of local centrality scores at a distance 4 is unlikely to be informative if most of the nodes are connected to most other nodes at this distance.

The degree, therefore, is a measure of local centrality, and a comparison of the degrees of various nodes in a graph can show how well connected the nodes are with their local environments.

This measure of local centrality has one major limitation. That is comparisons of centrality scores can only meaningfully be made among members of the same graph or between graphs that are the same size. The degree of a node depends on, among other things, the size of the graph, and so measure of local centrality cannot be compared when graphs differ significantly in size.

Local centrality is, however, only one conceptualization of node centrality, and Freeman (1979, 1980) has proposed a measure of global centrality based around what he terms the closeness of the nodes.

A degree-based measure of point centrality can be extended beyond direct connections to those at various path distances. In this case, the relevant 'neighbourhood' is widened to include the more distant connections of the points. A point may, then, he assessed for its local centrality in terms of both direct (distance 1) and distance 2 connections or, indeed, whatever cut-off path distance is chosen. The principal problem with extending this measure of point centrality beyond distance 2 connections is that, in graphs with even a very modest density, the majority of the points tend to be linked through indirect connections at relatively short path distances. Thus, comparisons of local centrality wares at distance 4, for example, are [EN 87] unlikely to be informative if most of the points are connected to

[p. 84]

most other points at this distance. [...] The degree, therefore, is a measure of local centrality, and a comparison of the degrees of the various points in a graph can show how well connected the points are with their local environments.

This measure of local centrality has, however, one major limitation. This is that comparisons of centrality mores can only [EN 88] meaningfully be made among the members of the same graph

[p. 85]

or between graphs which are the same size. The degree of a point depends on, among other things, the size of the graph, and so measures of local centrality cannot be compared when graphs differ significantly in size. [...] Local centrality is, however, only one conceptualization of point centrality, and Freeman (1979, 1990) has proposed a measure of **global centrality** based around what he terms the 'closeness' of the points.

[EN 87] [Bibliography is not available online] [EN 88]

Anmerkungen

Scott is mentioned in the thesis for the first time on page 220.

[128.] Nm/Fragment 103 15

Verschleierung

Untersuchte Arbeit: **Seite: 103, Zeilen: 15-27**	**Quelle: Koschuetzki_etal_2005** **Seite(n): 22-23, Zeilen: p22: 12ff; p23: 1-3**
We denote the sum of the distances from a vertex u ∈ V to any other vertex in a graph G = (V,E) as the total distance $\sum_{v \in V} d(u,v)$.	We denote the sum of the distances from a vertex u ∈ V to any other vertex in a graph G = (V,E) as the total distance [FN 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. [...]
The problem of finding an appropriate location can be solved by computing the set of vertices with a 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 more 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 structural index.	In our sense this definition is a vertex centrality, since cC(u) grows with decreasing total distance of u and it is clearly a structural index.

Farbig

Anmerkungen

The source is not mentioned anywhere in the thesis

[129.] Nm/Fragment 104 02

Verschleierung

Untersuchte Arbeit: **Seite: 103, Zeilen: 2-8**	**Quelle: Stephenson and Zelen 1989** **Seite(n): 3, Zeilen: 10-16**
The third measure is called betweenness and is the frequency at which a node occurs on a geodesic that connects a pair 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” (Frantz, T. and K. M. Carley, 2005).	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).

Farbig

Anmerkungen

nothing is marked as a citation, the source remains unnamed.

[130.] Nm/Fragment 104 12

Verschleierung

Untersuchte Arbeit:
Seite: 104, Zeilen: 12-24

Quelle: Koschuetzki_etal_2005
Seite(n): 29-30, Zeilen: p29: 26ff; p30: 1, 13-15

Farbig

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 s and t. 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.

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 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:

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

[...]

[...] 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 thesis anywhere.

Telling mistake: indeed, in his definition Nm writes "where σ_{uw} denotes the number of all shortest-paths between s and t.", thus mistakenly referring to the name of the nodes in the original text.

[131.] Nm/Fragment 106 14

Verschleierung

Untersuchte Arbeit:
Seite: 106, Zeilen: 14-17

Quelle: Balasundaram et al 2006
Seite(n): 2, Zeilen: 39-43

Farbig

The Figure 1.4 (in Chapter 1) shows an example of a terrorist network, which maps the links between terrorists involved in the tragic events of September 11, 2001. This graph was constructed by Valdis Krebs (2002) using the public data that were available [before, but collected after the event.]

Figure 1 shows an example of a terrorist network, which maps the links between terrorists involved in the tragic events of September 11, 2001. This graph was

constructed in [32] using the public data that were available before, but collected after the event.

---

[32]. Krebs, V.: Mapping networks of terrorist cells. Connections 24, 45–52 (2002)

Anmerkungen

To be continued on the next page Nm/Fragment_107_01

[132.] Nm/Fragment 107 01

KomplettPlagiat

Untersuchte Arbeit: **Seite: 107, Zeilen: 1-4**	**Quelle: Balasundaram et al 2006** **Seite(n): 2, Zeilen: 41-45** Farbig
[This graph was constructed by Valdis Krebs (2002) using the public data that were available] before, but collected after the event. Even though the information mapped in this network is by no means complete, its analysis may still provide valuable insights into the structure of a terrorist organization.	This graph was constructed in [32] using the public data that were available before, but collected after the event. Even though the information mapped in this network is by no means complete, its analysis may still provide valuable insights into the structure of a terrorist organization. [32]. Krebs, V.: Mapping networks of terrorist cells. Connections 24, 45–52 (2002)

Anmerkungen

The copied text starts on the previous page: Nm/Fragment_106_14

[133.] Nm/Fragment 107 07

Verschleierung

Untersuchte Arbeit: Seite: 107, Zeilen: 7-23	Quelle: Penzar_etal_2005 Seite(n): 33-34, Zeilen: 2ff; 1ff	Farbig
According to Kreb's (2002) analysis, this network had 62 members in total, of which 19 were kidnapers, and 43 assistants: organizers, couriers, financiers, scouts, representatives, coordinators, counterfeiters, etc. Allen (2004) found that successfully functioning large networks typically comprise 25-80 members, with an optimal size between 45 and 50. A close match exists between the results of Allen's analysis of collaborating networked groups and this particular example of a terrorist group. Inspection of this network by standard measures of network structure reveals firstly its low connectedness. A member of this network holds only 4.9 connections with others members on average (also known as degree centrality), which means that average members were rather isolated from the rest of the network. The density (which is defined as the number of actual links divided by the number of possible links) of this network is only 0.08, meaning that only 8% of all possible connections in the network really exist.	According to Krebs' analysis, this wider network had 62 members in total, of which 19 were kidnappers, and 43 assistants: organisers, couriers, financiers, scouts, counterfeiters etc. Allen found that successfully functioning large networks typically comprise 25-80 members, with optimal size between 45 and 50. Again, a close match exists between the results of Allen's analysis of collaborating networked groups and this particular example of a terrorist group. [Page 34] Inspection of this network by standard measures of network structure [16 – 18] reveals firstly its low connectedness. A member of this network holds only 4,9 connections with other members on average [En 3], which means that average members are rather isolated from the rest of the network. [...] Connectedness measure [EN 4] of this network is only 0,08, meaning that only 8 % of all possible connections in the network really exist. --- [EN 3] This means that average degree of nodes is 4,9, where degree of a node represents the number of links coming out of the node. [EN 4] Connectedness of a given network is the ratio of actually existing number of links in this network and the maximal number of links that would be possible in a network with the same number of nodes, where each node would be linked to each other. --- [16] Krebs, V.E.: An Introduction to Social Network Analysis. 2005, http://www.orgnet.com /sna.html, [17] Wolfe, A.W.: Applications of Network Models – Glossary to Accompany the Course and the Manuscript. 2001, http://luna.cas.usf.edu /~wolfe/glossary.html, [18] Borgatti, S.P.: Intra-Organizational Networks. Handouts for the course Introduction to Organizational Behavior, 1996, revised 2002, http://www.analytictech.com /mb021/intranet.htm,	

Anmerkungen

There is no reference to the source.

Note, that at the beginning of chapter 3 on page 93, there is a footnote commenting the title of chaper 3. It says:

FN 13: The parts of this chapter are already published in (Memon N, Henrik, L. L. 2006a, 2006b, 2006c, 2006d)

However, the source Penzar et al. (2005) has been published before any of those publications.

[134.] Nm/Fragment 108 02

Verschleierung

Untersuchte Arbeit: **Seite: 108, Zeilen: 2-19**	**Quelle: Penzar_etal_2005** **Seite(n): 34, Zeilen: 8ff**
In spite of low connectedness, however, the nodes of this network are relatively close. The average closeness of nodes is 0.35. Betweenness as stated above is another important measure in SNA and it indicates a node's importance for communication among other nodes. The average betweenness of this network is 0.032, indicating relatively high average redundancy. However the betweenness of 40 nodes is in fact less than 1% and only 6 nodes have betweenness higher than 10%. These 6 nodes are critical for information flow, especially one with betweenness of almost 0.589, meaning that almost 60% of communication paths among other nodes pass through this central node. The node represents Mohamed Atta (node # 33); the leading organizer of the attack whose central position in the network is confirmed by other centrality indicators as well. Distribution of degrees of nodes (see Section 3.4.1) is particularly interesting. Degrees of nodes are exponentially distributed: the degree of most of the nodes is small, while few nodes have high degree (see Figure 3.5 and Figure 3.6).	In spite of the low connectedness, however, nodes of this network are relatively close. [...] the average closeness [EN 5] of nodes is 0,35. Betweenness [FN 6] is another important measure in social network analysis and it indicates a node's importance for communication among other nodes. The average betweenness of this network is 0,032, indicating relatively high average redundancy. However, betweenness of forty nodes is in fact less than 1 %, and only six nodes have betweenness higher than 10 %. These six nodes are obviously critical for information flow, especially the one with betweenness of almost 60 %, meaning that almost 60 % of communication paths among other nodes pass through this central node. This node represents Mohamed Atta, the leading organiser of the attack whose central position in the network is confirmed by other centrality indicators as well. [...] Distribution of degrees of nodes is particularly interesting. Degrees of nodes are exponentially distributed: the degree of most nodes is small, while only few nodes have high degree (Fig. 6).

Farbig

Anmerkungen

There is no reference to the source.

Note, that at the beginning of chapter 3 on page 93, there is a footnote commenting the title of chaper 3, which says:

FN 13: The parts of this chapter are already published in (Memon N, Henrik, L. L. 2006a, 2006b, 2006c, 2006d)

However, the source Penzar et al. (2005) has been published before any of those publications.

[135.] Nm/Fragment 109 01

Verschleierung

Untersuchte Arbeit: Seite: 109, Zeilen: 1-13	Quelle: Penzar_etal_2005 Seite(n): 34, 35, Zeilen: 25ff; 4ff	Farbig

[This property characterises] the so called scale free networks (Watts, D.J., 2003; Kreisler, H., 2003). Scale free networks (see Section 3.5) form spontaneously, without needing a particular plan or interventions of central authority. Nodes that are members of the network for a longer time, that are better connected with other nodes, and that are more significant for a functioning network, are also more visible to new members, so that the new members spontaneously connect more readily to such nodes than other, relatively marginal ones.

[FIGURE: identical to corresponding figure in Source]

Figure 3.6. Distribution of degree of nodes in the network (see Figure 1.4) of kidnappers and their supporters.

On the pattern of scale free networks, the Al Qaeda's Training Manual (2001) states: "The cell or cluster methods should be organized in a way that a group is composed of many cells whose members do not know each other, so that if a cell member is caught, other cells would not be affected, and work would proceed [normally".]

This property characterises the so-called scale-free networks [19, 20; pp.104-111][EN 8], [...]. Scale-free networks form spontaneously, without needing a particular plan or interventions of a central authority. Nodes that are members of the network for a longer time, that are better connected with other nodes, and that are more significant for network's functioning, are also more visible to new members, so that the new members spontaneously connect more readily to such nodes than to other, relatively marginal ones.

[FIGURE]

Figure 6. Distribution of degrees of nodes in the network of kidnappers and their supporters

[Page 35]

[...] Al-Qaeda's Training Manual states: "Cell or cluster methods should be adopted by the Organization. It should be composed of many cells whose members do not know one another, so that if a cell member is caught, the other cells would not be affected, and work would proceed normally." [12; Third Lesson].

---

[12] Al Qaeda Training Manual. US Department of Justice, http://www.usdoj.gov/ag/ trainingmanual.htm and http://www.pbs.org /wgbh/pages/ frontline/shows/network/alqaeda/manual.html,

[18] Borgatti, S.P.: Intra-Organizational Networks. Handouts for the course Introduction to Organizational Behavior, 1996, revised 2002, http://www.analytictech.com/ mb021/intranet.htm,

[19] Li, L.; Anderson, D.; Tanaka R.; Doyle J.C.; Willinger, W.: Towards a Theory of Scale- Free Graphs: Definition, Properties, and Implications. Technical Report CIT-CDS-04-006, Engineering and Applied Sciences Division, California Institute of Technology, Pasadena, 2004, http://arxiv.org/PS_cache/ cond-mat/pdf/0501/0501169.pdf,

[20] Watts, D.J.: Six Degrees – The Science of a Connected Age. W. W. Norton & Company, New York, London, 2003,

Anmerkungen

There is no reference to the source.

Note, that at the beginning of chapter 3 on page 93, there is a footnote commenting the title of chaper 3. It says:

FN 13: The parts of this chapter are already published in (Memon N, Henrik, L. L. 2006a, 2006b, 2006c, 2006d)

However, the source Penzar et al. (2005) has been published before any of those publications.

[136.] Nm/Fragment 111 17

KomplettPlagiat

Untersuchte Arbeit: **Seite: 111, Zeilen: 17-27**	**Quelle: Holmgren 2006** **Seite(n): 956, Zeilen: right column 18-32** Farbig
In graph theory a number of measures have been proposed to characterize networks. However, three concepts are particularly important in contemporary studies of the topology of complex networks: degree distribution, clustering coefficient, and average path length (Albert, R., and Barabasi, A.L. (2002); Dorogovtsev, S. N., and Mendes, J. F. F. (2002); Newman, M. E. J. (2003)).	In graph theory, a number of measures have been proposed to characterize networks. However, three concepts are particularly important in contemporary studies of the topology of complex networks: degree distribution, clustering coefficient, and average path length. [EN 1-3]
3.4.1 Degree Distribution	*2.2.1. Degree Distribution*
The degree k_i is the number of edges connecting to the ith vertex. The vertex degree is characterized by a distribution function *P(k)*, which gives the probability that a randomly selected vertex has *k* edges. Recent studies show that several complex networks have a [heterogeneous topology, i.e., some vertices have a very large number of edges, but the majority of the vertices only have a few edges.]	The degree k_i is the number of edges connecting to vertex i. The vertex degree is characterized by a distribution function *P(k)*, which gives the probability that a randomly selected vertex has *k* edges. Recent studies show that several complex networks have a heterogeneous topology, i.e., some vertices have a very large number of edges, but the majority of the vertices only have a few edges.
	[EN 1]. Albert, R., & Barabási, A.-L. (2002). Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74, 47–97.
	[EN 2]. Dorogovtsev, S. N., & Mendes, J. F. F. (2002). Evolution of networks. *Advances in Physics*, 51, 1079–1187.
	[EN 3]. Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review*, 45, 167–256.

Anmerkungen

Nearly identical, though the source is not mentioned anzwhere.

[137.] Nm/Fragment 112 01

KomplettPlagiat

Untersuchte Arbeit:
Seite: 112, Zeilen: 1-27

Quelle: Holmgren 2006
Seite(n): 956-957, Zeilen: p.956, right column 28-45 - p.957, left column 1-18

Farbig

[Recent studies show that several complex networks have a] heterogeneous topology, i.e., some vertices have a very large number of edges, but the majority of the vertices only have a few edges. That is, the degree distribution follows a power law $P(k) \cup k^{-\gamma}$ for large *k*(i.e., $P(k)/k^{-\gamma} \to 1$ when $k \to \infty$). The average degree *(k)* of a graph with *N* vertices and *M* edges is *(k) = 2M / N*.

3.4.2 Clustering Coefficient

Many complex networks exhibit an inherent tendency to cluster. In social networks this represents a circles of friends in which every member knows each other. The clustering coefficient is a local property capturing “the density” of triangles in a graph, i.e., two vertices that both are connected to a third vertex are also directly connected to each other. An i^{th} vertex in a network has k_i edges that connects it to k_i other vertices. The maximum possible number of edges between the k_i neighbours is $\binom{k_i}{2} = k_i(k_i-1)/2$. The clustering coefficient of i^{th} vertex is defined as the ratio between the number M_i of edges that actually exist between these k_i vertices and the maximum possible number of edges, i.e., $C_i = 2M_i/k_i(k_i-1)$. The clustering coefficient of the whole network

$$C = (1/N)\sum_{i=1}^{n} C_i \sum_{i=1}^{n} C_i$$

3.4.3 Average Path Length

The distance l_{uv} between two vertices *u* and *v* is defined as the number of edges along the shortest path connecting them. The average path length $l = (l_{uv}) = [1/N(N-1)] \sum_{u \neq v \in V} l_{uv}$ is a measure of how a network is scattered. Sometimes, the diameter *d* of a graph is defined as the maximum path length between any two connected vertices in the graph. However, in other situations the concept diameter relate to the average path length, i.e., *d = l*.

[p. 956]

Recent studies show that several complex networks have a heterogeneous topology, i.e., some vertices have a very large number of edges, but the majority of the vertices only have a few edges. That is, the degree distribution follows a power law $P(k) \cup k^{-\gamma}$ for large *k*(i.e., $P(k)/k^{-\gamma} \to 1$ when $k \to \infty$). The average degree *(k)* of a graph with *N* vertices and *M* edges is *(k) = 2M/N*.

2.2.2. Clustering Coefficient

Many complex networks exhibit an inherent tendency to cluster. In social networks this represents circles of friends in which every member knows each other. The clustering coefficient is a local property capturing “the density” of triangles in the graph, i.e., two vertices that both are connected to a third vertex are also directly connected to each other. A vertex *i* in the network has k_i edges that connects it to

[p. 957]

k_i other vertices. The maximum possible number of edges between the ki neighbors is $\binom{k_i}{2} = k_i(k_i-1)/2$. The clustering coefficient of vertex *i* is defined as the ratio between the number M_i of edges that actually exist between these k_i vertices and the maximum possible number of edges, i.e., $C_i = 2M_i/k_i(k_i-1)$. The clustering coefficient of the whole network $C = (1/N)\sum_i C_i$.

2.2.3. Average Path Length

The distance l_{uv} between two vertices *u* and *v* is defined as the number of edges along the shortest path connecting them. The average path length $l = (l_{uv}) = [1/N(N-1)] \sum_{u \neq v \in V} l_{uv}$ is a measure of how the network is scattered. Sometimes, the diameter *d* of a graph is defined as the maximum path length between any two connected vertices in the graph. However, in other situations the concept diameter relate to the average path length, i.e., *d = l*.

Anmerkungen

The copying process continues with Nm introducing an unfortunate mistake in the formula for the clustering coefficient. Apart from this mistake, both texts are nearly identical.

[138.] Nm/Fragment 113 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 113, Zeilen: 1-22	Quelle: Holmgren 2006 Seite(n): 957, Zeilen: left column 18-42	Farbig

[The] so-called small-world property appears to characterize many complex networks. Despite their often-large size, there is a relatively short path between any two vertices in a network: the average shortest paths between a pair of vertices scales as the logarithm of the number of vertices.

3.5 GRAPHS AS MODELS OF REAL-WORLD NETWORKS

The study of networks, and in particular the interest in the statistical measures of the topology of networks (see section 3.4), has given birth to three main classes of network models. The *random graph* was introduced by Erdos and Renyi in the late 1950s and is one of the earliest theoretical models of a network (Bollobas, B., 1985). This is the easiest model to analyze mathematically and it can serve as a reference for randomness. Watts and Strogatz introduced the so called *small world model* in 1998 (Watts, D. J., and Strogatz, S. H., 1998). This model combines high clustering and a short average path length.

In 1999, Barabasi and Albert (BA) addressed the origin of the power-law degree distribution, evident in many real networks, with a simple model (also known as the *scale-free network model*) that put the emphasis on how real networks evolve (Albert, R., Jeong, H., and Barabasi, A.L., 2000).

The so-called small-world property appears to characterize many complex networks. Despite their often-large size, there is a relatively short path between any two vertices in the network: the average shortest paths between

a pair of vertices scales as the logarithm of the number of vertices.

2.3. Graphs as Models of Real-World Networks

2.3.1. Theoretical Network Models

The study of networks, and in particular the interest in the statistical measures of the topology of networks (previous section), has given birth to three main classes of network models. The *random graph* was introduced by Erdös and Rènyi in the late 1950s and is one of the earliest theoretical models of a network. [EN 12] This is the easiest model to analyze mathematically and it can serve as a reference for randomness. Watts and Strogatz introduced the so-called *small world model* in 1998. [EN 4] This model combines high clustering and a short average path length. In 1999, Barabási and Albert (BA) addressed the origin of the power-law degree distribution, evident in many real networks, with a simple model (also known as the *scale-free network* model) that put the emphasis on how real networks evolve. [EN 13]

[EN 4]. Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of "small-world" networks. *Nature*, 393, 440–442.

[EN 12]. Bollobás, B. (1985). *Random Graphs*. London: Academic Press.

[EN 13]. Albert, R., Jeong, H., & Barabási, A.-L. (2000). Error and attack tolerance of complex networks. *Nature*, 406, 378–382.

Anmerkungen

The third page of text which is identical to Holmgren (2006). No source given.

[139.] Nm/Fragment 113 23

Verschleierung

Untersuchte Arbeit: Seite: 113, Zeilen: 23-27	Quelle: Chen 2006 Seite(n): 98, Zeilen: 34-37	Farbig

Three models have been used to distinguish complex networks: *random graph model*, *small-world model*, and *scale-free model* (Albert and Barabasi, 2002). It is to note that most complex systems are not random but are governed by some well known principles encoded in the topology of the networks.

Three models have been employed to characterize complex networks: random graph model, small-world model, and scale-free model (Albert & Barabasi, 2002). Most complex systems are not random but are governed by certain organizing principles encoded in the topology of the networks.

Anmerkungen

Nm writes sentences that can also be found in a book of one of Nm's referees.

Moreover, in view of what Nm has written in the previous paragraphs the first sentence with its reference does not make much sense, since it is more or less a repetition of a list given further above.

[140.] Nm/Fragment 114 01

Verschleierung

Untersuchte Arbeit: Seite: 114, Zeilen: 1-12	Quelle: Chen 2006 Seite(n): 98-99, Zeilen: p.98,37-39 - p.99,1-8
It is worthwhile to mention here, that a small-world network has a significantly larger clustering coefficient while the network has small average path length. The large clustering coefficient point outs that there is a high tendency for nodes to form communities and groups. On the other hand, scale-free networks are characterized by the power-law degree distribution, meaning that while a large number of nodes in the network have just a few links, a small fraction of the nodes have a large number of links. It is believed that scale-free networks evolve following the selforganizing principle, where growth and preferential attachment play a key role for the emergence of the power law degree distribution (Chen, Hsinchun, 2006).	[p. 98] A small-world network has a significantly larger clustering coefficient than its random model counterpart while maintaining a relatively small average path [p. 99] length. The large clustering coefficient indicates that there is a high tendency for nodes to form communities and groups. Scale-free networks, on the other hand, are characterized by the power-law degree distribution, meaning that while a large number of nodes in the network have just a few links, a small fraction of the nodes have a large number of links. It is believed that scale-free networks evolve following the self-organizing principle, where growth and preferential attachment play a key role for the emergence of the power-law degree distribution.

Farbig

Anmerkungen

It is not clear that this paragraph is an - if you know the source - obvious citation. The reference "(Chen, Hsinchun, 2006)" indeed refers to one possible source at hand even though it is a multi authored paper (the wording is close to the one in Chen's book, which is presented here).

Chen was one of the referees for this thesis, so one expects that he, at least, is - more or less - correctly cited. This is not the case.

[141.] Nm/Fragment 114 13

Verschleierung

Untersuchte Arbeit: Seite: 114, Zeilen: 13-19	Quelle: Chen 2006 Seite(n): 98, Zeilen: 23-28
Although the topological properties of these networks have been discovered, the structures of terrorist networks are largely unknown due to the difficulty of collecting and accessing reliable data (Krebs, 2001). Do terrorist networks share the same topological properties with other types of networks? Do they follow the same organizing principle? How do they achieve efficiency under constant surveillance and threat from authorities? (Chen, Hsinchun, 2006).	Although the topological properties of these networks have been discovered, the structures of dark (covert, illegal) networks are largely unknown due to the difficulty of collecting and accessing reliable data (Krebs, 2001). Do dark networks share the same topological properties with other types of networks? Do they follow the same organizing principle? How do they achieve efficiency under constant surveillance and threat from authorities?

Farbig

Anmerkungen

Straight from the book of one of the referees, but the citation is not marked as such. The reference is to one of the papers of the referee, but the wording is nearly identical to what can be found in the book.

[142.] Nm/Fragment 114 20

BauernOpfer

Untersuchte Arbeit: Seite: 114, Zeilen: 20-33	Quelle: Krebs 2004 Seite(n): 1 (internet version), Zeilen: 38-47
This study applied the small-world network metrics of Watts & Strogatz (1998) to Figure 1.4 and tabulated in Table 3.1. One of the key metrics in the small-world model is the average path length, for individuals and for the network overall (Krebs, V., 2005). A good score for an individual means that he/she is close to all of the others in a network – they can reach others quickly without going through too many intermediaries. A good score for the whole network indicates that everyone can reach everyone else easily and quickly. The shorter the information paths for everyone, the quicker the information arrives and the less distorted it is when it arrives. Another benefit of multiple short paths is that most members of the network have good visibility into what is happening in other parts of the network – a greater awareness. They have a wide network horizon which is useful for combining key pieces of distributed [intelligence.]	We apply the small-world network metrics of Watts & Strogatz to Figures 1, 2, and 3 above. One of the key metrics in the small-world model is the average path length, for individuals and for the network overall. A good score for an individual means that he/she is close to all of the others in the network -- they can reach others quickly without going through too many intermediaries. A good score for the whole group indicates that everyone can reach everyone else easily and quickly. The shorter the information paths for everyone, the quicker the information arrives and the less distorted it is when it arrives. Another benefit of multiple short paths is that most members of the network have good visibility into what is happening in other parts of the network. They have a good network horizon which is useful for combining key pieces of distributed intelligence.

Farbig

Anmerkungen

Taken straight from the world wide web; the reference is given - still it is by no means clear that it mostly is a word-for-word citation. Note also that the copied text continues after the reference to the source.

[143.] Nm/Fragment 115 01

BauernOpfer

Untersuchte Arbeit: Seite: 115, Zeilen: 1-3	Quelle: Krebs 2004 Seite(n): 1 (internet version), Zeilen: 47-48
In an environment where it is difficult to distinguish signal from noise, it is important to have many perspectives involved in the sense-making process (Krebs, V., 2005).	In an environment where it is difficult to distinguish signal from noise, it is important to have many involved in the sense-making process.

Farbig

Anmerkungen

source given, but the citation is not marked as such; continuation from the previous page

[144.] Nm/Fragment 115 04

Verschleierung

Untersuchte Arbeit: Seite: 115, Zeilen: 4-10	Quelle: Chen 2006 Seite(n): 99-100, Zeilen: p.99,39-42 - p.100,1.4.
It would be noted that this research study found that members in the 9/11 terrorist network (Figure 1.4) are extremely close to their leaders. The terrorists in the network are on average only 1.79 steps away from Mohamed Atta, meaning that Mohammed Atta's (node 33) command can reach an arbitrary member through only two mediators (approximately). Despite its small size (62), the average path length is 3.01, [...]	[p. 99] We found that members in the criminal and terrorist networks are extremely close to their leaders. The terrorists in the GSJ network are on average only 2.5 steps away from bin Laden, meaning that bin Laden's command can reach an arbitrary member [p.100] through only two mediators. [...] Despite its small size (80), the average path length is 4.70, [...]

Farbig

Anmerkungen

different example, but the words are in large parts identical to a section in one of Nm's referees' book.

[145.] Nm/Fragment 115 12

BauernOpfer

Farbig

Untersuchte Arbeit: Seite: 115, Zeilen: 12-23	Quelle: Qin et al 2005 Seite(n): 299, Zeilen: 1-8, 12-14
The other small-world topology, high clustering coefficient, is also present in this network. The clustering coefficient of this network is 0.49 significantly high. Previous studies have also shown the verification of groups in this network. In these groups, members be likely to have solid (dense) and stronger relations with one another. The communication between group members becomes more efficient, making a crime/ terrorist plan or an attack easier to plan, organize, and execute (Chen, Hsinchun, 2006). In addition, this type of network is a scale-free system (as discussed above). The degree distribution decays slowly for small degrees than for that of other types of networks, which indicates a higher frequency for small degrees.	The other small-world topology, high clustering coefficient, is also present in the GSJ network (see Table 2). The clustering coefficient of the GSJ network is significantly higher than its random graph counterpart. Previous studies have also shown the evidence of groups and teams inside this kind of illegal networks [12, 33, 43, 44]. In these groups and teams, members tend to have denser and stronger relations with one another. The communication between group members becomes more efficient, making an attack easier to plan, organize, and execute [27]. Moreover, the GSJ network is also a scale-free system. [...] The degree distribution decays much more slowly for small degrees than for that of other types of networks, indicating a higher frequency for small degrees.

Anmerkungen

different example, but the words are in large parts identical

[146.] Nm/Fragment 117 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 117, Zeilen: 1-2, 3-8	Quelle: Chen 2006 Seite(n): 98, Zeilen: 29-33
The topological properties of 9/11 terrorist network is reported in the table above. [...] It is hoped that this study not only to contribute to general knowledge of the topological properties of complex systems (particularly terrorist networks) in a hostile environment but also to provide law enforcement and intelligence agencies with insights regarding destabilizing strategies strategies.	We report in this study the topological properties of several covert criminal- or terrorist-related networks. We hope not only to contribute to general knowledge of the topological properties of complex systems in a hostile environment but also to provide authorities with insights regarding disruptive strategies.

Anmerkungen

Taken out of context and put at the end of his own example of research.

[147.] Nm/Fragment 118 08

BauernOpfer

Untersuchte Arbeit: Seite: 118, Zeilen: 8, 12-25	Quelle: Latora and Marchiori 2004 Seite(n): 70, Zeilen: 4, 9-10, 18-19, 23-24, 27-31

Farbig

3.6.1 The Efficiency of a Network

[...] (Latora and Marchiori, 2004). The network efficiency *E(G)* is a measure to quantify how efficiently the nodes of a network exchange information. To define efficiency of a network *G*, first we calculate the shortest path lengths d_{ij} between the i^{th} and the j^{th} nodes. Let us now suppose that every node sends information along the network, through its links. The efficiency in the communication between the i^{th} node and the j^{th} node is inversely proportional to the shortest distance: when there is no path in the graph between the i^{th} and the j^{th} nodes, we get $d_{ij} = +\infty$ and efficiency becomes zero. Let *N* be known as the size of the network or the numbers of nodes in the graph, the average efficiency of the graph (network) of *G* can be defined as:

$$C_{eff} = E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \quad (6)$$

The above formula gives a value of $C_{eff} E$ in the interval of [0, 1].

2. The efficiency of a network

[...]

The *network efficiency E*, is a measure introduced in Refs. [5,6] to quantify how efficiently the nodes of the network exchange information.

[...]

To define the efficiency of **G** first we have to calculate the shortest path lengths $\{d_{ij}\}$ between two generic points *i* and *j*.

[...]

Let us now suppose that every vertex sends information along the network, through its edges. We assume that the efficiency ϵ_{ij} in the communication between vertex *i* and *j* is inversely proportional to the shortest distance: [...] when there is no path in the graph between *i* and *j* we get $d_{ij} = +\infty$ consistently $\epsilon_{ij} = 0$. Consequently the average efficiency of the graph **G** can be defined as [12]:

$$E(\mathbf{G}) = \frac{\sum_{i \neq j \in G} \epsilon_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}. \quad (1)$$

Such a formula (1) gives a value of *E* that can vary in the range $[0, \infty[$,

[...]

Anmerkungen

Though the source is given, there is no hint that the text following the reference is taken nearly word-for-word from the source (with some shortening). Also, it makes no sense to speak of the "ith" and "jth" node as there is no linear order on a graph. The nodes are just referred to as "i" and "j", as in the source.

At the end, Nm produces a mathematical mistake by leaving out too much.

[148.] Nm/Fragment 125 01

BauernOpfer

Untersuchte Arbeit: Seite: 125, Zeilen: 1-29	Quelle: Wikipedia_Riyadh_compound_bombings_2007 Seite(n): 1 (internet version), Zeilen: -- Farbig
3.7.2 Case 2: Riyadh Bombing Terrorists Network [FN 19]	**Riyadh compound bombings**
The Riyadh bombings took place on May 12, 2003, in Riyadh, Saudi Arabia. The bombing involved suicide attacks, attributed to Al Qaeda, were the first of several "spectacular attacks" carried out by that group in 2003, and reported as the terrible attack on Americans that year. In the attack 35 people were killed, and over 160 injured.	From Wikipedia, the free encyclopedia The Riyadh compound bombings took place on May 12, 2003, in Riyadh, Saudi Arabia. These suicide attacks, attributed to al-Qaeda, were the first of several "spectacular attacks" carried out by that group in 2003, and the deadliest attack on Americans that year. Altogether, some 35 people were killed, and over 160 wounded.
It is reported that on May 12, when much of Riyadh was asleep, four vehicles drove through Riyadh (two cars, a pickup, and an SUV). Two carried heavily armed assault teams and three of them were packed with explosives. Their targets were three compounds: *The Dorrat Al Jadawel*, the *Al Hamra Oasis Village*, and the *Vinnell Corporation Compound*. It is very important to point that all compounds contained large numbers of Americans and Westerners.	[...] Late on May 12, while much of Riyadh was asleep, four vehicles drove through Riyadh; two cars, a pickup, and an SUV. Two carried heavily armed assault teams and three of them were packed with explosives. Their targets were three compounds: The Dorrat Al Jadawel, a compound owned by MBI International and Partners, the Al Hamra Oasis Village, and the Vinnell Corporation Compound, a compound owned by a Virginia-based defense contractor that was training the Saudi National Guard. All contained large numbers of Americans and Westerners.
It is reported that around 11:15 PM, a car packed with explosives and five or six terrorists, attempted to enter to the Jadawel compound's back gate area. As the guards approached to check the vehicle, the terrorists abruptly opened fire, killing one Saudi Air Force policeman and one un-armed Saudi civilian security guard. The attackers' bunched gunfire violently as they attacked the inner compound gate, injuring two other security guards, one of whom managed to secure the gates before fleeing. While the terrorists were still attempting to get inside the compound, their massive explosive suddenly exploded as reported on the media, killing all of the terrorists and a Filipino worker.	Around 11:15 PM, a car packed with explosives and five or six terrorists, quietly attempted to gain entry to the Jadawel compound's back gate area. As the guards approached to inspect the vehicle, the terrorists suddenly opened fire, immediately killing one Saudi Air Force policeman and one unarmed Saudi civilian security guard. The attackers sprayed gunfire wildly as they assaulted the inner compound gate, wounding two other unarmed security guards, one of whom managed to secure the gates before fleeing. While the terrorists were still attempting to get inside the compound, their massive explosive charge suddenly detonated, killing all of the attackers and a Filipino worker.
At the Al Hamra Oasis Village and the Vinnell Corp. compound, the terrorists shot the security guards outside the compound gates. After that they opened the gates with the security controls and a second team of terrorists drove their trucks into the compounds.	At the Al Hamra Oasis Village and the Vinnell Corp. compound, the assault teams shot the security guards outside the compound gates. They then opened the gates with the security controls and a second team drove their trucks into the compounds.
--- [FN 19] The most of the text is taken from http://en.wikipedia.org /wiki/Riyadh_Compound_Bombings	

Anmerkungen

"most of" appears to mean that everything on this page has been taken from the Wikipedia entry as existed on 11 February 2007 with only some phrases and words having been changed by Nm

[149.] Nm/Fragment 126 01

BauernOpfer

Untersuchte Arbeit: Seite: 126, Zeilen: 1-10	Quelle: Wikipedia_Riyadh_compound_bombings_2007 Seite(n): 1 (internet version), Zeilen: 16ff Farbig
[As] they fired roughly, they shouted phrases like "God is Great!". Then they exploded both of their bombs, destroying the compounds.	As they fired wildly, they screamed phrases like "God is Great!". They then detonated both of their bombs, devastating the compounds.
It was reported that at least 26 people died, including 09 US citizens. The fatalities contained seven Saudis, three Filipinos, two Jordanians, and one each from Australia, Britain, Ireland, Lebanon and Switzerland.	Altogether at least 26 people died, including nine Americans. The nationalities of the other dead were seven Saudis, three Filipinos, two Jordanians, and one each from Australia, Britain, Ireland, Lebanon and Switzerland. In addition, nine suicide bombers died, bringing the entire toll from the attacks to 35. More than 160 other people were injured, including more than two dozen Americans.
It was also mentioned that, nine suicide bombers died, bringing the entire fatalities from the attacks to 35. In the incident more than 160 other people were injured, including more than two dozen US Citizens.	

Anmerkungen

continuation from previous page

[150.] Nm/Fragment 138 12

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 138, Zeilen: 12-20	Quelle: Freeman 1980 Seite(n): 587, Zeilen: 17-24
Consider a network representing a symmetrical relation, “communicates with” for a set of nodes. When a pair of nodes (say, *u* and *v*) is linked by an edge so that they can communicate directly without intermediaries, they are said to be adjacent. A set of edges linking two or more modes (*u*, *v*, *w*) such that *u* would like to communicate with *w*, using node *v*, then how many times node *u* uses node *v* to reach node *w* and how many shortest paths node *u* uses to reach node *w*. There can, of course, be more than one geodesic, linking any pair of nodes.	Consider a graph representing the symmetrical relation, "communicates with" for a set of people. When a pair of points is linked by an edge so that they can communicate directly without intermediaries, they are said to be adjacent. A set of edges linking two or more points (p_i, p_j, p_k) such that p_i is adjacent to p_j and p_j is adjacent to p_k constitute a path from p_i to p_k. The shortest path linking a pair of points is called a geodesic. There can, of course, be more than one geodesic linking any pair of points.

Anmerkungen

A barely concealed mostly verbatim adaption of what can be found in Freeman (1980). Where Nm leaves the path of the original text the definition becomes nearly incomprehensible and mathematically unsound (although the definition of a path given by Freeman also leaves a bit to be desired).

[151.] Nm/Fragment 139 11

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 139, Zeilen: 11-14	Quelle: Freeman 1980 Seite(n): 588, Zeilen: 1-4
The dependence centrality is defined 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 [...]	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, [...]

Anmerkungen

The interpretation of the mathematical definitions is word-for-word the same (although the definitions differ actually).

[152.] Nm/Fragment 140 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 140, Zeilen: 1-6	Quelle: Freeman 1980 Seite(n): 588, Zeilen: 10-14
Each entry in *D* is an index of the degree to which the node designated by the row of a 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 gatekeeper with respect to every other node—facilitating 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.

Anmerkungen

Even though nearly identical, a reference to the source is completely missing.

[153.] Nm/Fragment 143 02

Verschleierung

Untersuchte Arbeit: Seite: 143, Zeilen: 2-5	Quelle: Stephenson and Zelen 1989 Seite(n): 26-27, Zeilen: p.26,36-37 - p.27,1	Farbig
Above Section proposed, developed and illustrated a new measure of centrality called dependence centrality, which may be applied to terrorist networks. This measure reflects the information contained in the shortest paths in a network.	[page 26] We have proposed, developed and illustrated by the use of examples a new measure of centrality called information, which may be applied to [page 27] nondirected networks. This measure reflects the information contained in all possible paths in a network.	

Anmerkungen

adapted to fit the theme of the thesis, otherwise identical; nothing is marked as a citation, no reference given.

[154.] Nm/Fragment 144 13

KomplettPlagiat

Untersuchte Arbeit: Seite: 144, Zeilen: 13-15	Quelle: Stephenson and Zelen 1989 Seite(n): 27, Zeilen: 34-36	Farbig
This chapter attempted to illustrate the calculation of centralities to these prototypical situations. However we regard our efforts in this direction as only a beginning.	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

This piece is taken word-for-word from the conclusion of the paper which functioned as an unreferenced source. The sentences following will be taken from one of the second of the paper's introductory chapters.

[155.] Nm/Fragment 144 16

KomplettPlagiat

Untersuchte Arbeit: Seite: 144, Zeilen: 16-21	Quelle: Stephenson and Zelen 1989 Seite(n): 3, Zeilen: 28-33	Farbig
It is possible that information will take a more circuitous route either by random communication or may be intentionally channelled 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.	

Anmerkungen

This is supposed to be a part of a summary, which Nm did for this chapter. But in fact it stems verbatim from the unnamed source. This section will appear a second time in Nm's thesis as Nm/Fragment_242_09.

[156.] Nm/Fragment 146 03

Verschleierung

Untersuchte Arbeit: Seite: 146, Zeilen: 3-15	Quelle: Penzar_etal_2005 Seite(n): 28, Zeilen: 2-12
After tragic terrorist attacks by hijacked airlines on New York and Washington in September 2001 the interest for Al Qaeda in public and media rose immediately. Experts and analysts all over the world started to offer various explanations of Al Qaeda's origins, membership recruitment, modes of operation, as well as of possible ways of its disruption. Journalists in search of hot topics took over and publicized most of the publicly available materials, often revising them further and making them even more exciting and attractive for wide audiences. One could thus read or hear that Al Qaeda is "a net that contains independent intelligence", that it "functions as a swarm", that it "gathers from nowhere and disappears after action", that it is "an ad hoc network", "an atypical organization", extremely hard to destroy, especially by traditional anti-terrorist or counterterrorist methods.	After catastrophic terrorist attacks by kidnapped airlines on New York and Washington in September 2001 the interest for al-Qaeda terrorist organisation in public and media rose immediately. Experts and analysts all over the world started to offer various explanations of al-Qaeda's origins, membership recruitment, modes of operation, as well as of possible ways of its disruption. Journalists in search of hot topics took over and publicized most of the publicly available materials, often revising them further and making them even more intriguing and attractive for wide audiences. One could thus read or hear that al-Qaeda is "a net that contains independent intelligence", that it "functions as a swarm", that it "gathers from nowhere and disappears after action", that it is "an ad hoc network", "an atypical organisation", extremely hard to destroy, especially by traditional anti-terrorist methods.

Farbig

Anmerkungen

Very minor changes. No reference to the source.

Note FN 22 (commenting the title of chapter 5): "The parts of this chapter are already published in Memon N., Larsen Henrik Legind 2006c, 2006d, 2007c and Memon N., Qureshi A.R. (2005)." However, Penzar et al. (2005) has been received in May 2005, Memon & Quereshi (2005) has been published in November,

[157.] Nm/Fragment 146 20

Verschleierung

Untersuchte Arbeit: Seite: 146, Zeilen: 20-25	Quelle: Combating Terrorism Center 2006 Seite(n): 8, Zeilen: 14-18
Al Qaeda has evolved from a centrally directed organization into a worldwide franchiser of terrorist attacks (Grier P., 2005). Since war in Afghanistan, which significantly degraded Osama bin Laden's command and control, Al Qaeda does appear to have become increasingly decentralized. It is now seen by many as more of a social [movement than coherent organization (Wikotorowicz Q., 2001).]	According to most counterterrorism analysts today, al-Qa'ida has evolved from a centrally directed organization into a worldwide franchiser of terrorist attacks. [FN 7] Indeed, since the war in Afghanistan, which significantly degraded bin Laden's command and control, al-Qa'ida has become increasingly decentralized, and is seen by some as more of a "movement" than any other form of organization. [FN 7] Peter Grier, "The New Al Qa'ida: Local Franchiser," *Christian Science Monitor* (11 July 2005). Online at: http://www.csmonitor.com /2005/0711/p01s01-woeu.html.

Farbig

Anmerkungen

The source is dated February 14, 2006. According to Nm [FN 22] "parts of this chapter are already published in Memon N., Larsen Henrik Legind 2006c, 2006d, 2007c and Memon N., Qureshi A.R. (2005)." This section appeared in Memon N., Larsen Henrik Legind 2006c in the Proceedings of the second International Conference, ADMA 2006, which was held in August 2006. Thus the unnamed source predates the writing of this section of Nm's thesis.

[158.] Nm/Fragment 147 01

BauernOpfer

Untersuchte Arbeit:
Seite: 147, Zeilen: 1-13

[It is now seen by many as more of a social] movement than coherent organization (Wikotorowicz Q., 2001).

Al Qaeda did not decide to decentralize until 2002, following the removal of the Taliban from Afghanistan and the arrest of a number of key Al Qaeda leaders including Abu Zubaydhah, Al Qaeda's Dean of students, Ramzi bin Al Shibh, the organizer of the Hamburg cell of 9/11 hijackers, Khalid Sheikh Mohammed, the mastermind of 9/11 and the financier of the first World Trade Center attack, and Tawfiq Attash Kallad, the master mind of the USS Cole attack.

In response these and other key losses, Al Qaeda allegedly convened a strategic summit in northern Iran in November 2002, at which the group's consultative council decided that it could no longer operate as a hierarchy, but instead would have to decentralize (Joseph Felter et al., 2005).

Quelle: Combating Terrorism Center 2006
Seite(n): 8, Zeilen: p.8,17-18 and p.9,14-19.20-21.23-24.25-26.26-29

Farbig

[p. 8]

[...] and is seen by some as more of a "movement" than any other form of organization.

[...]

[p. 9]

Indeed, several years ago al-Qa'ida's leaders recognized that the achievement of their ultimate goals and objectives required a more decentralized, networked approach. In 2001, following the ouster of the Taliban from Afghanistan, a number of al-Qa'ida leaders suddenly found themselves in detention centers facing long months of interrogation. Abu Zubaydah, al-Qa'ida's "dean of students," [...]. Ramzi Bin al Shibh, the organizer of the Hamburg, Germany cell that formed the core of the 9/11 hijackers, [...] Khalid Sheik Mohammed, the mastermind of 9/11 and the financier of the first World Trade Center attack, [...] Tawfiq Attash Kallad, the mastermind of the USS Cole attack, [...] In response to the loss of key leaders, al-Qa'ida allegedly convened a strategic summit in northern Iran in November 2002, at which the group's consultative council came to recognize that it could no longer exist as a hierarchy, but instead would have to become a decentralized network [...][FN 10]

[FN 10] Robert Windrem, 2005.

Anmerkungen

In spite of some paraphrasing this remains a collage of various bits and pieces of various lengths from the unnamed source from West Point's Combating Terrorism Center. Nothing is marked as a citation.

Both sources, (Wikotorowicz Q., 2001) as well as (Joseph Felter et al., 2005) are not to be found in Nm's list of references. However, "Felter et al. 2005" might refer to a version of the source, as "Joe Felter" led its large team of authors.

[159.] Nm/Fragment 147 18

Verschleierung

Untersuchte Arbeit: Seite: 147, Zeilen: 18-29	Quelle: Yang_etal_2005 Seite(n): 2, Zeilen: 8ff	Farbig
Hierarchy, as one common feature of many real world networks, attracts special attentions in recent years (Ravasz, E., A. L., Barabasi, 2003; Costa, L. D. F., 2004; Trusina, A. et al, 2004, Variano, E. A. et al, 2004). Hierarchy is one of the key aspects of a theoretical model to capture statistical characteristics of terrorist networks. In literature, several concepts are proposed to measure the hierarchy in a network, such as the hierarchical path (Trusina, A. et al, 2004), the scaling law for the clustering coefficients of nodes in a network (Ravasz, E., A. L., Barabasi, 2003), etc. These measures can tell us the existence and extent of hierarchy in a network. We address herein another problem how to construct hidden hierarchy of terrorist networks (which are known as horizontal networks).	Hierarchy, as one common feature for many real world networks, attracts special attentions in recent years [9-12]. [...] Hierarchy is one of the key aspects of a theoretical model [9,13] to capture the statistical characteristics of a large number of real networks, [...] In literature, several concepts are proposed to measure the hierarchy in a network, such as the hierarchical path [10], the scaling law for the clustering coefficients of the nodes [9], the hierarchical components/degree [11], etc. These measures can tell us the existence and the extent of hierarchy in a network. We address herein another problem, that is, how to reconstruct the hierarchical structure in a network. --- [9] E. Ravasz and A. -L. Barabasi, Phys. Rev. E 67, 026112(2003). [10] A. Trusina, S. Maslov, P. Minnhagen and K. Sneppen, Phys. Rev. Lett. 92, 178702(2004). [11] L. D. F. Costa, Phys. Rev. Lett. 93, 098702(2004). [12] E. A. Variano, J. H. McCoy and H. Lipson, Phys. Rev. Lett. 92,188701(2004). [13] Tao Zhou, Gang Yan and Binghong Wang, Phys. Rev. E 71, 046141 (2005).	

Anmerkungen

Only minor adjustments. In particular also all the literature references are taken from Yang et al. (2005).

Note: the footnote 22, commenting the title of chapter 5 on page 146, reads as follows: "22 The parts of this chapter are already published in Memon N., Larsen Henrik Legind 2006c, 2006d, 2007c and Memon N., Qureshi A.R. (2005)." However, Memon N., Qureshi A.R. (2005) was published in November 2005 (see here (http://www.worldses.org/journals/computers/computers-november2005.doc)), whereas Yang et al (2005) was published in August 2005.

[160.] Nm/Fragment 162 03

Verschleierung

Untersuchte Arbeit: Seite: 162, Zeilen: 3-8	Quelle: Krebs 2002 Seite(n): 46, Zeilen: 9-15	Farbig
Osama Bin Laden's strategy, which he described in famous videotape which was found in a hastily deserted house in Afghanistan. In the transcript (Department of Defense), Laden mentions that "*Those who were trained to fly didn't know the others. One group of people did not know the other group.*"	Usama bin Laden even described this strategy on his infamous video tape which was found in a hastily deserted house in Afghanistan. In the transcript (Department of Defense, 2001) bin Laden mentions: *Those who were trained to fly didn't know the others. One group of people did not know the other group.*	

Anmerkungen

No reference given.

[161.] Nm/Fragment 165 01

Verschleierung

Untersuchte Arbeit: Seite: 165, Zeilen: 1, 3-6	Quelle: Latora and Marchiori 2004 Seite(n): 73, Zeilen: 16, 17-18
In this case study we consider the connections network of terrorists involved in the Bali Night Club Bombing and their directed or undirected relationships with other entities. Of course mapping networks after an event is relatively easy, while the real problem in this case is to map the covert networks to prevent terrorist activity, a task that can be more difficult.	As a second example we consider the connections network of the hijackers and related terrorists of the September 2001 attacks. Of course mapping networks after an event is relatively easy, while the real problem in this case is to map covert networks to prevent criminal activity, a task that can be much more difficult.

Farbig

Anmerkungen

Nearly identical at the end but nothing is marked as a citation; the reference is not given.

[162.] Nm/Fragment 166 11

KomplettPlagiat

Untersuchte Arbeit: Seite: 166, Zeilen: 11-18	Quelle: WorldNetDaily - Wheeler 2003 Seite(n): 1 (internet version), Zeilen: --
Shukrijumah is believed to be working on Osama bin Laden's plan to trigger a radiological disaster inside the United States – the so-called "dirty-bomb" scenario where a small charge would trigger dispersion of radiation over a large area, causing chaos on those caught in the blast and making the blast area uninhabitable. It is to mention that the high-grade uranium is not necessary for this project; ordinary, low-grade nuclear waste will be deadly enough.	Adnan El Shukrijumah [...] He is believed to be working on Osama bin Laden's plan to trigger a radiological disaster inside the United States – the so-called "dirty-bomb" scenario where a small charge would trigger dispersion of radiation over a large area, wreaking havoc on those caught in the blast and making the blast area uninhabitable. High-grade uranium is not necessary for this project; ordinary, low-grade nuclear waste will be deadly enough.

Farbig

Anmerkungen

The source is not named; the phrasing in the source Wikipedia given in footnote 27 5 lines earlier on the first mention of the name Shukrijumah does not match.

[163.] Nm/Fragment 168 03

KomplettPlagiat

Untersuchte Arbeit: Seite: 168, Zeilen: 3-13	Quelle: Wikipedia - Adnan Gulshair el Shukrijumah - 2006 Seite(n): 1 (internet version), Zeilen: 3rd paragraph
It is believed by authorities that Shukrijumah may have been trained at an Al Qaeda terrorist camp. Shukrijumah has extensive flight training that he received at a flight school in Florida and is a pilot, though he is not registered with the Federal Aviation Administration (FAA). Apparently, this is of concern to law enforcement since practically all the Al Qaeda hijackers involved in the September 11 terrorist attacks, received training to be pilots at U.S. private flight schools. It is also believed by the FBI, that Shukrijumah has been trained by Al Qaeda to operate as a terrorist organizer and operational / field commander and lead or coordinate a terrorist assault, in much the [same way that Mohammed Atta was designated and trained as an organizer and operational/field leader by Al Qaeda to lead the September 11 hijackers in killing 3,100 by attacking The Pentagon in Arlington, Virginia and leveling the World Trade Center in Manhattan, New York City, New York.]	It is believed by authorities that Shukrijumah may had been trained at an al-Qaida terrorist camp. Shukrijumah has extensive flight training that he received at a flight school in Florida and is a pilot, though he is not registered with the Federal Aviation Administration (FAA). Obviously, this is of concern to law enforcement since virtually all the al-Qaida hijackers involved in the September 11 terrorist attacks, received training to be pilots at U.S. private flight schools. Also, it is believed by the FBI that Shukrijumah has been trained by al-Qaida to operate as a terrorist organizer and opeartional/field commander and lead or coordinate a terrorist assault, much the same way Mohammed Atta was designated and trained as an organizer and operational/field leader by al-Qaida to lead the September 11 hijackers in killing 3,100 by attacking The Pentagon in Arlington, Virginia and leveling the World Trade Center in Manhattan, New York City, New York.

Farbig

Anmerkungen

Several pages earlier Nm named http://en.wikipedia.org/wiki/Adnan_el-Shukrijumah as the source for his information on Shukrijumah. He did not mention that further on one would find a nearly identical copy of the original text in this thesis.

[164.] Nm/Fragment 169 01

Verschleierung

Untersuchte Arbeit:
Seite: 169, Zeilen: 1-10

Quelle: Wikipedia - Adnan Gulshair el Shukrijumah - 2006
Seite(n): 1 (internet version), Zeilen: --

Farbig

[It is also believed by the FBI, that Shukrijumah has been trained by Al Qaeda to operate as a terrorist organizer and operational / field commander and lead or coordinate a terrorist assault, in much the] same way that Mohammed Atta was designated and trained as an organizer and operational/field leader by Al Qaeda to lead the September 11 hijackers in killing 3,100 by attacking The Pentagon in Arlington, Virginia and leveling the World Trade Center in Manhattan, New York City, New York. It is obvious that El Shukrijumah may play a large and leading role in the next set of terrorist attacks to come upon the U.S. It is reported that Shukrijumah was last seen in the Miami or southern Florida area in the early part of 2003. He has not been seen since and no one knows of his whereabouts till the publication of this dissertation.

Also, it is believed by the FBI that Shukrijumah has been trained by al-Qaida to operate as a terrorist organizer and opeartional/field commander and lead or coordinate a terrorist assault, much the same way Mohammed Atta was designated and trained as an organizer and operational/field leader by al-Qaida to lead the September 11 hijackers in killing 3,100 by attacking The Pentagon in Arlington, Virginia and leveling the World Trade Center in Manhattan, New York City, New York. El Shukrijumah may play a large and leading role in the next set of terrorist attacks to come upon the U.S. [...] Shukrijumah was last seen in the Miami or southern Florida area in the early part of 2003. He has not been seen since and no one knows of his whereabouts.

Anmerkungen

continued from previous page

Nm draws his information concerning the whereabouts of El Shukrijumah from Wikipedia only (without telling anybody).

[165.] Nm/Fragment 170 02

BauernOpfer

Untersuchte Arbeit:
Seite: 170, Zeilen: 2-7

Quelle: Wikipedia - World Trade Center bombing (1993) - 2006
Seite(n): 1 (internet version), Zeilen: --

Farbig

5.4.3 WTC 1993 Bombing Plot[FN 28]

The WTC bombing attack in the garage occurred on February 26, 1993 of the New York World Trade Center. A car bomb was planted by terrorist groups in the underground parking garage below tower One. It is reported that the attack killed six, and injured over 1,000 and gave indication for the 9/11 attacks on the same buildings.

The World Trade Center bombing was the February 26, 1993, terrorist attack in the garage of the New York City World Trade Center. A car bomb was detonated by Arab Islamist terrorists in the underground parking garage below Tower One. It killed six, injured over 1,000, and presaged the September 11, 2001, terrorist attacks on the same buildings.

[FN 28] http://en.wikipedia.org/wiki/World_Trade_Center_bombing

Anmerkungen

The original has only been slightly adapted. Large subsentences were left unchanged and would have required citation.

[166.] Nm/Fragment 171 01

BauernOpfer

Farbig

Untersuchte Arbeit: Seite: 171, Zeilen: 1-4	Quelle: Wikipedia - World Trade Center bombing (1993) - 2006 Seite(n): 1 (internet version), Zeilen: --
Ramzi Yousef began in 1991 to plan a bombing attack at USA. Yousef's Uncle Khalid Shaikh Mohammed gave him advice and tips over the phone, and funded him. Yousef entered the USA with a false passport in 1992.	Ramzi Yousef, born in Kuwait, began in 1991 to plan a bombing attack within the United States. Yousef's uncle Khalid Shaikh Mohammed, [...] gave him advice and tips over the phone, and funded him with a US$660 wire transfer.[FN 1] Yousef entered the United States with a false Iraqi passport in 1992.

Anmerkungen

slightly shortened but still extremely close to the original.

The source is given on the previous page.

[167.] Nm/Fragment 174 02

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 174, Zeilen: 2-16	Quelle: Wikipedia-Bojinka-plot_2006 Seite(n): 1, Zeilen: 1ff
Oplan Bojinka was a planned large scale attack on airliners in 1995. It is reported that the term refers to "airline bombing plot" alone, or that combined with the "Pope assassination plot" and the "CIA plane crash plot". The first ("airline bombing plot") refers to a plot to destroy 11 airliners on January 21 and 22, 1995, the second ("Pope assassination plot") refers to a plan to kill Pope John Paul II on January 15, 1995, and the third ("CIA plane crash plot".) refers a plan to crash a plane into the CIA headquarters in Fairfax County, Virginia and other buildings. Oplan Bonjika was prevented on January 6, and 7, 1995, but some lessons learnt were apparently used by the planners of the September 11 attacks. It is also reported that the money that funded operation Bojinka came from Osama Bin Laden and (R. Isamuddin) Hambali, and also from organizations operated by Jamal Khalifa, Bin Laden's brother in law.	**Oplan Bojinka** [...] was a planned large-scale attack on airliners in 1995, [...]. The term can refer to the "airline bombing plot" alone, or that combined with the "Pope assassination plot" and the "CIA plane crash plot". The first refers to a plot to destroy 11 airliners on January 21 and 22, 1995, the second refers to a plan to kill Pope John Paul II on January 15, 1995, and the third refers a plan to crash a plane into the CIA headquarters in Fairfax County, Virginia and other buildings. Oplan Bojinka was prevented on January 6 and 7, 1995, but some lessons learned were apparently used by the planners of the September 11 attacks. [...] The money that funded Operation Bojinka came from Osama bin Laden and Hambali, and from front organizations operated by Mohammed Jamal Khalifa, bin Laden's brother-in-law.

Anmerkungen

The source is not mentioned.

[168.] Nm/Fragment 178 05

Verschleierung

Untersuchte Arbeit: Seite: 178, Zeilen: 5-15	Quelle: Perer_Shneiderman_2006 Seite(n): 693, Zeilen: -	Farbig
Social network analysis (SNA) has emerged as a powerful method for understanding the importance of relationships in networks. However, interactive exploration of networks is currently challenging because: (1) it is difficult to find patterns and comprehend the structure of networks with many nodes and links, and (2) current systems are often a combination of statistical methods and overwhelming visual output which leaves many analysts uncertain about how to explore in an orderly manner. This results in exploration that is largely opportunistic. Our contributions are techniques to help intelligence analysts understand social terrorist networks more effectively.	Abstract— Social network analysis (SNA) has emerged as a powerful method for understanding the importance of relationships in networks. However, interactive exploration of networks is currently challenging because: (1) it is difficult to find patterns and comprehend the structure of networks with many nodes and links, and (2) current systems are often a medley of statistical methods and overwhelming visual output which leaves many analysts uncertain about how to explore in an orderly manner. This results in exploration that is largely opportunistic. Our contributions are techniques to help structural analysts understand social networks more effectively	

Anmerkungen

Almost 1-to-1 copy of the first part of the abstract of Perer & Shneiderman (2006). One of the few changes has been to introduce the word "terrorist".

The source is not given.

[169.] Nm/Fragment 180 02

Verschleierung

Untersuchte Arbeit: Seite: 180, Zeilen: 2-16	Quelle: Perer_Shneiderman_2006 Seite(n): 693, Zeilen: -	Farbig
6.2 EXPLORING TERRORIST NETWORKS Understanding networks is a basically a difficult process. It is difficult to visualize, navigate, and most problematic, to detect patterns in terrorist networks. Despite all of these challenges, the network perspective is appealing. It is to mention that network analysts also focus on relationships instead of just the individual nodes (like we did in this study); putting nodes together is just as important as the nodes themselves. Before to this perspective, social research focused largely on attributes and neglected the social part of behaviour (how individuals interact and the influence they have on each other) (Freeman L. C., 2004). Using techniques from the social network community, analysts can easily find patterns in the structure, witness the flow of resources through a network, and learn how individuals are influenced by their surroundings.	Understanding networks is an inherently difficult process. It is difficult to visualize, navigate, and most problematic, find patterns in networks. Despite all of these challenges, the network perspective is appealing. Network analysts focus on relationships instead of just the individual elements; how the elements are put together is just as important as the elements themselves. Prior to this perspective, social research focused largely on attributes and neglected the social part of behavior (how individuals interact and the influence they have on each other) [EN 12]. Using techniques from the social network community, analysts can find patterns in the structure, witness the flow of resources through a network, and learn how individuals are influenced by their surroundings. [EN 12] L. C. Freeman, The Development of Social Network Analysis: A Study in the Sociology of Science, Empirical Press, 2004.	

Anmerkungen

Only minor changes. The source is not given anywhere in the thesis. The source pages are not numbered, this is in the first column of the first page.

[170.] Nm/Fragment 181 01

Verschleierung

Untersuchte Arbeit: **Seite: 181, Zeilen: 1-33**	**Quelle: Perer_Shneiderman_2006** **Seite(n): 693, Zeilen: left column, 2nd paragraph ff** Farbig
In practice, a network visualization of a domain can be a messy one, particularly when the network is very large. Visualizations are useful to influence the powerful perceptual skills of humans, but overlapping links and labels of nodes mostly weaken this approach. It is to note that say that I cannot say researchers studying networks are completely lost. The techniques from sociology to graph theory in the literature can be found that allow analysts to detect interesting structures in networks. Analysts might pursue a tight-coupled community of the actors, or the brokers between them, or the most powerful actors – and there are a number of complex algorithms for detecting these behaviours.	In practice, a network visualization of a domain can be a messy one, particularly when the network is large. Visualizations are useful to leverage the powerful perceptual abilities of humans, but overlapping links and illegible labels of nodes often undermine this approach. This is not to suggest that researchers studying networks are completely lost. There is a rich history of techniques from sociology to graph theory that allow analysts to find interesting features in networks. Analysts might seek a tight-knit community of individuals, or the gatekeepers between them, or the most centrally powerful entities – and there are a variety of sophisticated algorithms for finding these traits.
It is worthwhile to mention that more mature fields in the area known as biology have developed techniques to train beginners and guarantee uniformity among analysts. The techniques are complete, so if two analysts are able to present with the same data, they most probably reach at the same conclusion. Though, in the social networks area, different networks are required to be analyzed in a different way. The wide spread of an epidemic among small towns is not necessarily the same as a spread of a business disaster on world markets (Watts D. J., 2003). From the above discussion, it is found that since there is no systematic way to understand networks; researchers need to be able to discover features to order to see patterns.	More mature fields, such as field biology, have developed systematic methods to train novices and ensure consistency among analysts. The methods are complete and repeatable, so if two analysts are presented with the same data, they should reach the same conclusion. However, in the social networks field, different networks need to be analyzed differently. The spread of an epidemic among villages is not necessarily the same as a spread of a financial crisis on world markets [34]. Since there is no systematic way to interpret networks, users need to be able to flexibly explore features to discover patterns.
Freeman proposes that social network analysts pursue to expose two types of patterns in networks: i) those that disclose subsets of nodes that are ordered into unified social communities, and ii) those that disclose subsets of nodes that occupy comparable social roles (Freeman L. C., 2004b). A lot of work has been carried over the 6-7 decades to discover such patterns. Social Network Analysis: Methods and Applications, by Wasserman and Faust, is the main contribution used reference book for social scientists/ students (Wasserman S. and K. Faust, (1994). The book provides details and a review of SNA methods and description of the field.	[...] Freeman suggests that social network analysts seek to uncover two types of patterns in networks: (1) those that reveal subsets of nodes that are organized into cohesive social groups, and (2) those that reveal subsets of nodes that occupy equivalent social positions, or roles [FN 11]. There is a large body of work over the past 60 years to uncover such patterns. Social Network Analysis: Methods and Applications, by Wasserman and Faust, is perhaps the most widely used reference book for structural analysts [FN 33]. The book presents a review of network analysis methods and an overview of the field.

[FN 11] L. C. Freeman, "Graphic Techniques for Exploring Social Network Data", Models and Methods in Social Network Analysis, in P. J. Carrington, J. Scott and S. Wasserman, eds., Cambridge University Press, Cambridge, 2004

[FN 33] S. Wasserman and K. Faust, Social Network Analysis: Methods and Applications, Cambridge University Press, 1994.

[FN 34] D. J. Watts, Six Degrees: The Science of a Connected Age, W.W. Norton & Company, New York, 2003.

Anmerkungen

Slight modifications. Also literature references have been copied. The source is not given anywhere in the thesis.

Verschleierung

Untersuchte Arbeit:
Seite: 182, Zeilen: 1-33

It is to be noted that the visualizations of social networks have been used to support SNA from the beginning Freeman L. C., (2000). Visualization of networks is more important because it is a natural way to communicate connectivity and allows for fast pattern recognition by human eyes. On the contrary, there are a number of challenges when visualizing networks (Battista *et al*., 1999; Herman *et al*., 2000). A number of layout algorithms discuss how to calculate the position of each and every node and the curve of each link in order to minimize link crossings and observe to visual principles. The algorithms are not large in number, and it is very difficult if the notes are very large then visualization is very difficult (Ham F. van, 2005).

Numerous techniques try to use available display more proficiently by distorting the graph/ network. One of the popular techniques is fisheye technique, which allows users to observe a focus area in detail, For example, read for further details (Munzner T., (1997). Another technique is Multiscale graph abstraction that reserves global structure, but navigation became difficult because clusters are obviously contracted and expanded, more information can be found in (Auber, et al, 2003; Parker G., G. Franck and C. Ware, 1998). Recent work associates these two techniques with fisheyeviews to decrease the number of displayed nodes while protecting the network structure (Gansner, E. R., Y. Koren and S. North, 2005). In addition, Ham Van and Van Wijk (2004) also combine distortion strategies for highly connected small-world networks.

A number of software tools designed to assist analysts to understand social networks, such as (Borgatti, S., M. G. Everett and L. C. Freeman, 2006; Brandes, U. and D. Wagner, 2003; de Nooy W., A. Mrvar and V. Batageli, 2005). The tools offer exciting techniques that users can use on networks. Though, the techniques are mostly a combination of statistical methods and visual output that put many analysts unclear about in what way and how to discover in a systematic manner.

Quelle: Perer_Shneiderman_2006
Seite(n): 694, Zeilen: left column, 1ff

Farbig

Visualizations of social networks have been used to aid SNA from the beginning [EN 13]. The visualization of networks is important because it is a natural way to communicate connectivity and allows for fast pattern recognition by humans. However, there are great challenges when visualizing networks [EN 9, EN 18]. There are many layout algorithms that attempt to calculate the position of each node and the curve of each link to minimize link crossings and adhere to aesthetic principles. These algorithms fall short, however, when the number of nodes is larger than several hundred and the large number of overlapping links makes it hard to judge connectivity [EN 31].

Several approaches attempt to more efficiently use available display space by distorting the graph. Fisheye techniques allow users to examine a focus area in great detail, but also tend to obscure the global structure of networks, e.g. [EN 21, EN 23]. Multiscale graph abstraction is another technique that preserves global structure, however navigation is difficult because clusters are explicitly contracted and expanded, e.g. [EN 2, EN 26]. Recent work combines these two approaches with topological fisheye views to reduce the number of displayed nodes while preserving the network structure [EN 14]. Van Ham and van Wijk also combine distortion strategies for highly connected, small-world networks [EN 32].

There are a number of software tools designed to help analysts understand social networks, such as [5, 7, 8]. These tools often feature an impressive number of analysis techniques that users can perform on networks. However, they are also often a medley of statistical methods and overwhelming visual output that leaves many analysts uncertain about how to explore in an orderly manner.

[EN 2] D. Auber, Y. Chiricota, F. Jourdan and G. Melancon, "Multiscale Visualization of Small World Networks", IEEE Symposium on Information Visualization, pp. 75-81, 2003.

[EN 5] S. Borgatti, M. G. Everett and L. C. Freeman, UCINET 6, Analytic Technologies, 2006.

[EN 7] U. Brandes and D. Wagner, "visone - Analysis and Visualization of Social Networks", Graph Drawing Software,in M. Junger and P. Mutzel, eds., Springer-Verlag, 2003.

[EN 8] W. de Nooy, A. Mrvar and V. Batageli, Exploratory Social Network Analysis with Pajek, Cambridge University Press, Cambridge, 2005.

[EN 9] G. Di Battista, P. Eades, R. Tamassia and I. G. Tollis, Graph Drawing: Algorithms for the Visualization of Graphs, Prentice Hall, New Jersey, 1999.

[EN 13] L. C. Freeman, "Visualizing Social Networks", Journal of Social Structure, 2000.

[EN 14] E. R. Gansner, Y. Koren and S. North, "Topological Fisheye Views for Visualizing Large Graphs", IEEE Transactions on Visualization and Computer Graphics, 11, pp. 457-468, 2005.

[EN 18] I. Herman, G. Melancon and M. S. Marshall, "Graph visualization and navigation in information visualization: A survey", IEEE Transactions on Visualization and Computer Graphics, 6, pp. 23-43, 2000.

[EN 19] H. Kang, C. Plaisant, B. Lee and B. B. Bederson, "NetLens: Iterative Exploration of Content-Actor Network Data", IEEE Symposium on Visual Analytics Science and Technology, 2006.

[EN 21] J. Lamping and R. Rao, "The hyperbolic browser: A Focus+Context Technique for Visualizing Large Hierarchies", Journal of Visual Languages and Computing, 6, 1995.

[EN 23] T. Munzner, "H3: Laying Out Large Directed Graphs in 3D Hyperbolic Space", IEEE Symposium on Information Visualization, pp. 2-10, 1997.

Anmerkungen

Slight modifications. Also all literature references stem from the source, which is not given anywhere in the thesis. *et al* is sometimes in italics, sometimes not.

[172.] Nm/Fragment 183 01

Verschleierung

Untersuchte Arbeit: **Seite: 183, Zeilen: 1-14**	**Quelle: Perer_Shneiderman_2006** **Seite(n): 694, Zeilen: -** Farbig
[SNA is known as basically a] deductive assignment, and a user's investigative procedure can be confused by having to navigate between separate analysis and visualization packages.	SNA is an inherently deductive task, and a user's exploratory process can be distracted by having to navigate between separate analysis and visualization packages.
Most recently a number of projects focus to improve interactive exploration with networks. For example, *GUESS* is well known as a novel graph exploration system that combines an interpreted language with a graphical front end Adar E., (2006). *TreePlus* allows users to explore graphs using more comprehensible enhanced tree layouts (Lee, B. et al. 2006). *NetLens* allows users to discover an actor-event network using iterative queries and histograms (Kang, H. *et al* (2006). In addition, Ghoneim *et al*. (2004) presented matrix-based visualizations. *JUNG* is a JAVA toolkit which delivers analysts with a framework to construct their own SNA tools (O'Madadhain, J., 2005).	Recently, there have been several projects focusing on improving interactive exploration with networks. Among them, GUESS is a novel graph exploration system that combines an interpreted language with a graphical front end [EN 1]. TreePlus allows users to explore graphs using more comprehensible enhanced tree layouts [EN 22]. NetLens allows users to explore an actor-event network using iterative queries and histograms [EN 19]. Ghoneim et al. presented the promise of using matrix-based visualizations instead of node-link diagrams [EN 15]. JUNG is a JAVA toolkit that provides users with a framework to build their own social network analysis tools [EN 25].

[EN 1] E. Adar, "GUESS: A Language and Interface for Graph Exploration", ACM Conference on Human Factors in Computing Systems, 2006.

[EN 15] M. Ghoniem, J.-D. Fekete and P. Castagliola, "A Comparison of the Readability of Graphs Using Node-Link and Matrix-Based Representations", IEEE Symposium on Information Visualization, 2004.

[EN 19] H. Kang, C. Plaisant, B. Lee and B. B. Bederson, "NetLens: Iterative Exploration of Content-Actor Network Data", IEEE Symposium on Visual Analytics Science and Technology, 2006.

[EN 22] B. Lee, C. S. Parr, C. Plaisant, B. B. Bederson, V. D. Veksler, W. D. Gray and C. Kotfila, "TreePlus: Interactive Exploration of Networks with Enhanced Tree Layouts", IEEE Transactions on Visualization and Computer Graphics, 2006.

[EN 25] J. O'Madadhain, D. Fisher, P. Smyth, S. White and Y.-B. Boey, "Analysis and Visualization of Network Data using JUNG", Journal of Statistical Software, VV, 2005.

Anmerkungen

Minor adjustments, also literature references have been copied. The source is not given anywhere in the thesis.

[173.] Nm/Fragment 183 17

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 183, Zeilen: 17-24	Quelle: Heer et al 2005 Seite(n): 1 (internet version), Zeilen: 9-11, 13-20
Although information visualization (infovis) techniques prove to be vital tools for making sense of complex data. To report these issues, we have used Prefuse, a software framework for creating dynamic visualizations of both structured and unstructured data. The Prefuse provides theoretically-motivated abstractions for the design of a wide range of visualization applications, enabling programmers to string together desired components quickly to create and customize working visualizations.	Although information visualization (infovis) technologies have proven indispensable tools for making sense of complex data, wide-spread deployment has yet to take hold, [...] To address these issues, we have created *prefuse*, a software framework for creating dynamic visualizations of both structured and unstructured data. *prefuse* provides theoretically-motivated abstractions for the design of a wide range of visualization applications, enabling programmers to string together desired components quickly to create and customize working visualizations.

Anmerkungen

The source will be given later on with regard to the following paragraphs.

[174.] Nm/Fragment 183 25

BauernOpfer

Farbig

Untersuchte Arbeit: Seite: 183, Zeilen: 25-28	Quelle: Heer et al 2005 Seite(n): 3 (internet version), Zeilen: right column 17-20
6.3 DESIGN OF THE PREFUSE TOOLKIT [FN 31]	**DESIGN OF THE PREFUSE TOOLKIT**
In this Section the toolkit design (illustrated in Figure 6.2), presenting the architecture, basic abstractions, and provided libraries for processing and visualizing information is discussed.	We now describe the toolkit design (illustrated in Figure 2), presenting the architecture, basic abstractions, and provided libraries for processing and visualizing information.
[FN 31] The matter is taken from (Heer et al., 2005)	

Anmerkungen

Footnote 31 - indeed. In fact, already starting with the previous paragraph, there can be found nearly identical copies of large bodies of the original paper. This continues on the following pages of Nm's thesis.

However, Heer et al. is not listed in the bibliography.

[175.] Nm/Fragment 184 09

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 184, Zeilen: 9-11, 12-15	Quelle: Heer et al 2005 Seite(n): 3 (internet version), Zeilen: right column 34-36, 39-43
6.3.2 Filtering	**Filtering**
Filtering is the process of mapping abstract data to a representation suitable for visualization. [...] The corresponding visual analogues (called VisualItems) are generated, which, in addition to the attributes of the source data, record visual properties such as location, colour, and size. Individual filters are provided in [Prefuse as Action modules, discussed later in this section.]	Filtering is the process of mapping abstract data to a representation suitable for visualization. [...] Next, corresponding visual analogues (called VisualItems) are generated, which, in addition to the attributes of the source data, record visual properties such as location, color, and size. Individual filters are provided in prefuse as Action modules, discussed later in this section.

Anmerkungen

Starting with figure 6.2, which indeed is an exact copy (together with its caption) from Heer et al. (2005), after an "intermission" containing a paragraph which Nm seems to have authored himself (to paraphrase what could be found in the source), Nm continues his word-for-word "take-over" from Heer et al. (2005).

[176.] Nm/Fragment 185 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 185, Zeilen: 1-27	Quelle: Heer et al 2005 Seite(n): 3-4 (internet version), Zeilen: p. 3, right column 42-53 - p. 4 left column 1-16
[Individual filters are provided in] Prefuse as Action modules, discussed later in this section.	[p. 3] Individual filters are provided in prefuse as Action modules, discussed later in this section.
In the data state model of (Chi, E.H., 2000), filtering is made up of the *Visualization Transformation*: reducing abstract data to visualizable content. Filtering can also be understood as implementing a tiered version of the model-view-controller pattern (Krasner, G.E. and S.T. Pope, 1988). Abstract data provides a base model for any number of visualizations, while filtered data constitutes a visualization-specific model with its own set of view controllers. This enables multiple visualizations of a shared data set by using separate filters, and different views of a specific visualization by reusing the same filtered items, while isolating filtering logic away from the main application logic	In the data state model of [EN 15], filtering constitutes the *Visualization Transformation*: reducing abstract data to visualizable content. Filtering can also be understood as implementing a tiered version of the model-view-controller pattern [EN 29]. Abstract data provides a base model for any number of visualizations, while filtered data constitutes a visualization-specific model with its own set of viewcontrollers. This enables multiple visualizations of a shared data set by using separate filters, and different views of a specific visualization by reusing the same filtered items.
6.3.3 Managing Visual Items: The ItemRegistry	[p. 4]
Prefuse provides three types of VisualItem by default: NodeItems to visualize individual entities, EdgeItems to visualize relations between entities, and AggregateItems to visualize aggregated groups of entities. These items are arranged in a graph structure separate from the source data, maintaining a local version of the data topology and thereby enabling flexible representations of visualized content. If desired, additional VisualItem types can also be introduced.	**Managing Visual Items: The ItemRegistry** prefuse provides three types of VisualItem by default: NodeItems to visualize individual entities, EdgeItems to visualize relations between entities, and AggregateItems to visualize aggregated groups of entities. These items are arranged in a graph structure separate from the source data, maintaining a local version of the data topology and thereby enabling flexible representations of visualized content. If desired, additional VisualItem types can also be introduced.
VisualItems are recorded centrally in “ItemRegistry”. ItemRegisrty [sic!] data structure contains the overall state for a specific visualization. Filter Actions request visual analogues from the registry, which returns the VisualItems, creating them as needed. ItemRegistry can be viewed as a mapping between the abstract data and VisualItems. The ItemRegistry also contains a FocusManager.	VisualItems are created and stored in a centralized data structure called the ItemRegistry, which houses all the state for a specific visualization. Filter Actions request visual analogues from the registry, which returns the VisualItems, creating them as needed, and records the mapping between the abstract data and visualized content. The ItemRegistry also contains a FocusManager, [...]

	[EN 15] Chi, E.H. A Taxonomy of Visualization Techniques Using the Data State Reference Model. *InfoVis '00*. pp. 69-75 2000.
	[EN 29] Krasner, G.E. and S.T. Pope, A Description of the Model-View-Controller User Interface Paradigm in the Smalltalk-80 System. *Journal of Object-Oriented Programming*, 1988. 1(3): p. 26-49.

Anmerkungen

Continuation from previous page. A typo is to be found, where the text is not taken identically from the source. Interesting: a corresponding phrase in both texts (*Visualization Transformation*) is in italics.

[177.] Nm/Fragment 186 03

Verschleierung

Untersuchte Arbeit: **Seite: 186, Zeilen: 3-32**	**Quelle: Heer et al 2005** **Seite(n): 4, Zeilen: left column 24-38 - right column**

Farbig

To ensure performance, the ItemRegistry also recycles item instances when they are removed from the registry, avoiding object initialization costs that can cripple performance.

6.3.4 Actions

Actions are basic components of application design in Prefuse. Actions are composable processing modules that update the VisualItems in an ItemRegistry. Actions are the mechanism for selecting visualized data and setting visual properties, performing tasks such as filtering, layout, colour assignment, and interpolation. To facilitate extensibility, Actions follow a simple API: a single run method that takes an ItemRegistry and an optional fraction indicating animation progress as input. In addition, base classes for specific Action types such as filters and layout algorithms are provided. While Actions can perform arbitrary processing tasks, most fall into one of three types: filter, assignment, and animator actions. Filter actions performs tasks like filtering as described in previous subsections. Assignment actions are used to set attributes of VisualItems, for example: its position or colour. A variety of layout management techniques are also coded as actions in Prefuse. Animator actions interpolate visual attributes between starting and ending values to achieve animation, using the animation fraction provided by the Action interface. Prefuse includes animators for locations, colours, fonts, and sizes.

6.3.5 ActionLists and Activities

ActionLists are runnable routines which contain actions. A user may add as many Actions to ActionList as one wants. ActionList sequentially execute them as a sequential pipeline executing resources. These lists form processing pipelines that are invoked in response to user or system events. ActionLists are Actions themselves, allowing lists to be used as sub-routines of other lists [and recursion.]

To ensure performance, the ItemRegistry also recycles item instances when they are removed from the registry, avoiding object initialization costs that can cripple performance.

Actions

The basic components of application design in prefuse are Actions: composable processing modules that update the VisualItems in an ItemRegistry. Actions are the mechanism for selecting visualized data and setting visual properties, performing tasks such as filtering, layout, color assignment, and interpolation. To facilitate extensibility, Actions follow a simple API: a single run method that takes an ItemRegistry and an optional fraction indicating animation progress as input. In addition, base classes for specific Action types such as filters and layout algorithms are provided. While Actions can perform arbitrary processing tasks, most fall into one of three types: filter, assignment, and animator actions.

Filter actions perform the filtering process discussed earlier, controlling what entities and relations are represented by VisualItems in the ItemRegistry [...]

Assignment actions set visual attributes, such as location, color, font, and size, for VisualItems. prefuse includes extensible color, font, and size assignment functions and a host of layout techniques for positioning items.

Finally, *animator* actions interpolate visual attributes between starting and ending values to achieve animation, using the animation fraction provided by the Action interface. prefuse includes animators for locations, colors, fonts, and sizes.

ActionLists and Activities

To perform data processing, Actions are composed into runnable ActionLists that sequentially execute these Actions. These lists form processing pipelines that are invoked in response to user or system events. ActionLists are Actions themselves, allowing lists to be used as sub-routines of other lists.

Anmerkungen

Continuation from previous page. The second portion is marginally rewritten.

[178.] Nm/Fragment 187 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 187, Zeilen: 1-31	Quelle: Heer et al 2005 Seite(n): 4-5 (internet version), Zeilen: p.4,32-33 and p.5,1-30
ActionLists can be configured to run once, or to run periodically for a specified duration. The execution of ActionLists is managed by a general activity scheduler, implemented using the approach of (Hudson, S. and J.T. Stasko, 1993). The scheduler accepts Activity objects (a superclass of ActionList), parameterized by start time, duration, and step rate, and runs them accordingly. The scheduler runs in a dedicated thread and oversees all active Prefuse visualizations, ensuring atomicity and helping avoid concurrency issues. A listener interface enables other objects to monitor activity progress, and pacing functions (Hudson, S. and J.T. Stasko, 1993) can be applied to parameterize animation rates (*e.g.*, to provide slow-in slow-out animation). **6.3.6 Rendering and Display** Renderes draws VisualItems on the screen using the visual attributes of an item, for example, location, colour, to determine its actual on-screen appearance. Renderers have a simple API consisting of three methods: one to draw an item, one to return a bounding box for an item, and one to indicate if a given point is contained within an item. Prefuse includes Renderers for drawing basic shapes, straight and curved edges, text, and images, including image loading, scaling, and caching support. Implementing user can also define their own renders by extending existing Renderers, or by implementing the Renderer interface to implement custom behaviour. Mappings between items and appearances are managed by a RendererFactory: given a VisualItem, the RendererFactory returns an appropriate Renderer. This layer of indirection affords a high level of flexibility, allowing many simple Renderers to be written and then doled out as needed. It also allows visual appearances to be easily changed, either by issuing different Renderers in response [to data attributes, or by changing the RendererFactory for a given ItemRegistry.]	[p. 4] ActionLists can be configured to run once, or to run periodically for a specified duration. [p. 5] The execution of ActionLists is managed by a general activity scheduler, implemented using the approach of [EN 24]. The scheduler accepts Activity objects (a superclass of ActionList), parameterized by start time, duration, and step rate, and runs them accordingly. The scheduler runs in a dedicated thread and oversees all active prefuse visualizations, ensuring atomicity and helping avoid concurrency issues. A listener interface enables other objects to monitor activity progress, and pacing functions [EN 24] can be applied to parameterize animation rates (e.g., to provide slow-in slow-out animation). **Rendering and Display** VisualItems are drawn to the screen by Renderers, components that use the visual attributes of an item (e.g., location, color) to determine its actual on-screen appearance. Renderers have a simple API consisting of three methods: one to draw an item, one to return a bounding box for an item, and one to indicate if a given point is contained within an item. prefuse includes Renderers for drawing basic shapes, straight and curved edges, text, and images (including image loading, scaling, and caching support). Custom rendering can be achieved by extending existing Renderers, or by implementing the Renderer interface. Mappings between items and appearances are managed by a RendererFactory: given a VisualItem, the RendererFactory returns an appropriate Renderer. This layer of indirection affords a high level of flexibility, allowing many simple Renderers to be written and then doled out as needed. It also allows visual appearances to be easily changed, either by issuing different Renderers in response to data attributes, or by changing the RendererFactory for a given ItemRegistry. --- [En 24] Hudson, S. and J.T. Stasko. Animation Support in a User Interface Toolkit: Flexible, Robust, and Reusable Abstractions. *UIST'93*. pp. 57-67, 1993.

Anmerkungen

continued from previous page;

The whole page is a nearly left intact copy of material from Heer et al. (2005). The first sentence of 6.3.6 contains a typo, and that is in a part that was re-written.

[179.] Nm/Fragment 188 01

Verschleierung

Untersuchte Arbeit: Seite: 188, Zeilen: 1-30	Quelle: Heer et al 2005 Seite(n): 5 (internet version), Zeilen: left column 27-54 - right column 1-5

Farbig

[It also allows visual appearances to be easily changed, either by issuing different Renderers in response] to data attributes, or by changing the RendererFactory for a given ItemRegistry. This also provides a clean mechanism for semantic zooming (Perlin, K. and D. Fox, 1993) – the RendererFactory can select Renderers appropriate for the current scale value of a given display.

Display component presents the visualized data. Display acts as a camera onto the contents of an ItemRegistry. The Display is an extension of JComponent (Swing's base component), and thus can be used in any Java Swing application. The Display takes an ordered enumeration of visible items from the registry, applies view transformations, computes the clipping region, and draws all visible items using appropriate Renderers. The Java2D library is used to support affine transformations of the view, including panning and zooming and other animation strategies. ItemRegistry can be tied to multiple Displays, enabling multiple views. Displays support interaction with visualized items through a ControlListener interface, providing callbacks in response to mouse and keyboard events on items. Displays also provide direct manipulation textediting of item content and allow arbitrary Swing components to be used as interactive tooltips.

6.3.7 The Prefuse Library

Prefuse architecture is supported by a huge library, a bundle of default implementations and significant components. These components simplify application design by providing advanced functions frequently used in visualizations.

Layout and Distortion. Prefuse library contains a variety of implemented actions to manage layout and distortion techniques. Available layouts include random, circular, gridbased, forcedirected, top-down (Reingold, E.M. and J.S. Tilford, 1981), radial (Yee, K.-P., D. Fisher, R. Dhamija, and M.A. Hearst; 2001), [indented outline, and tree map [EN 32] (Bruls, M., K. Huizing, and J.J. van Wijk, 2000) algorithms.]

[EN 32] http://www.cs.umd.edu/hcil/treemap-history/

It also allows visual appearances to be easily changed, either by issuing different Renderers in response to data attributes, or by changing the RendererFactory for a given ItemRegistry. This also provides a clean mechanism for semantic zooming [EN 38] – the RendererFactory can select Renderers appropriate for the current scale value of a given Display.

Presentation of visualized data is performed by a Display component, which acts as a camera onto the contents of an ItemRegistry. The Display subclasses Swing's top-level JComponent, and can be used in any Java Swing application. The Display takes an ordered enumeration of visible items from the registry, applies view transformations, computes the clipping region, and draws all visible items using appropriate Renderers. The Java2D library is used to support affine transformations of the view, including panning and zooming. In addition, an ItemRegistry can be tied to multiple Displays, enabling multiple views (e.g., overview+detail [EN 12]).

Displays support interaction with visualized items through a ControlListener interface, providing callbacks in response to mouse and keyboard events on items. Displays also provide direct manipulation text-editing of item content and allow arbitrary Swing components to be used as interactive tooltips.

The prefuse Library

The core prefuse architecture described above is leveraged by a library of significant components. These components simplify application design by providing advanced functions frequently used in visualizations.

Layout and Distortion. prefuse is bundled with a library of Action modules, including a host of layout and distortion techniques. Available layouts include random, circular, gridbased, force-directed, top-down [EN 40], radial [EN 48], indented outline, and tree map [EN 10, EN 44] algorithms.

[EN 38] Perlin, K. and D. Fox. Pad: An Alternative Approach to the Computer Interface. *SIGGRAPH'93*. pp. 57-64, 1993.

[EN 12] Card, S.K., J.D. Mackinlay, and B. Shneiderman, *Readings in Information Visualization: Using Vision to Think*. San Francisco, California: Morgan-Kaufmann, 1999.

[EN 40] Reingold, E.M. and J.S. Tilford, Tidier Drawings of Trees. *IEEE Transactions of Software Engineering*, 1981. SE-7: p. 21-28.

[EN 48] Yee, K.-P., D. Fisher, R. Dhamija, and M.A. Hearst. Animated Exploration of Dynamic Graphs with Radial Layout. *InfoVis'01*. pp. 43-50 2001.

[EN 10] Bruls, M., K. Huizing, and J.J. van Wijk. Squarified TreeMaps. In *Proceedings of Joint Eurographics and IEEE TCVG Symp. on Visualization (TCVG 2000)*: IEEE Press. pp. 33-42, 2000.

[EN 44] Treemaps for Space-Constrained Visualization of Hierarchies. 1998. http://www.cs.umd.edu/hcil/treemap-history/

Anmerkungen

continued from previous page.

Also see Nm/Fragment 183 25 where the source is mentioned.

[180.] Nm/Fragment 189 01

Verschleierung

Untersuchte Arbeit:
Seite: 189, Zeilen: 1-29

[Available layouts include random, circular, gridbased, forcedirected, top-down (Reingold, E.M. and J.S. Tilford, 1981), radial (Yee, K.-P., D. Fisher, R. Dhamija, and M.A. Hearst; 2001),] indented outline, and tree map32 (Bruls, M., K. Huizing, and J.J. van Wijk, 2000) algorithms. These layouts are parameterized and reusable components. These facilitate the user to define their own new layouts by using existing modules. In addition, Prefuse supports space distortion of item location and size attributes, including graphical fisheye views (Sarkar, M. and M.H. Brown, 1992) and bifocal distortion (Leung, Y.K. and M.D. Apperley, 1992).

Force Simulation. Prefuse includes an extensible and configurable library for force-based physics simulations. This consists of a set of force functions, including n-body forces like gravity, spring forces, and drag forces. To support real-time interaction, n-body force calculations use the Barnes-Hut algorithm (Barnes, J. and P. Hut, 1986) to compute the otherwise quadratic calculation in log-linear time. The force simulation supports various numerical integration schemes. It is based on dynamic calculation of trade-offs in efficiency and accuracy, to update velocity and position values. These modules are based on numerical techniques like classic Runge-Kutta method. Again the design is flexible enough to accommodate the user defined extension to existing force based simulations.

Interactive Controls. Following the basic design of the Interactor paradigm (Myers, B.A., 1990), Prefuse includes parameterizable ControlListener instances for common interactions. It includes drag controls for repositioning VisualItems, focus controls for updating focus, navigation controls for panning and zooming, including both manual controls and speed-dependent automatic zooming (Igarashi, T. and K., 2000) and highlight settings in response to mouse actions and key press actions.

Quelle: Heer et al 2005
Seite(n): 5 (internet version), Zeilen: right column 3-30

Farbig

Available layouts include random, circular, gridbased, force-directed, top-down [EN 40], radial [EN 48], indented outline, and tree map [EN 10, EN 44] algorithms. These layouts are parameterized and reusable, hence one can write new layouts by composing existing modules. In addition, prefuse supports space distortion of item location and size attributes, including graphical fisheye views [EN 43] and bifocal distortion [EN 32].

Force Simulation. prefuse includes an extensible and configurable library for force-based physics simulations. This consists of a set of force functions, including n-body forces (e.g., gravity), spring forces, and drag forces. To support realtime interaction, n-body force calculations use the Barnes-Hut algorithm [EN 2] to compute the otherwise quadratic calculation in log-linear time. The force simulation supports various numerical integration schemes, with trade-offs in efficiency and accuracy, to update velocity and position values. The provided modules abstract the mathematical details of these techniques (e.g., 4th Order Runge-Kutta) from toolkit users. Users can also write custom force functions and add them to the simulator.

Interactive Controls. Inspired by the Interactor paradigm [EN 36], prefuse includes parameterizable ControlListener instances for common interactions. Provided controls include drag controls for repositioning items (or groups of items), focus controls for updating focus and highlight settings in response to mouse actions, and navigation controls for panning and zooming, including both manual controls and speeddependent automatic zooming [EN 25].

[EN 40] Reingold, E.M. and J.S. Tilford, Tidier Drawings of Trees. *IEEE Transactions of Software Engineering*, 1981. **SE-7**: p. 21-28.

[EN 48] Yee, K.-P., D. Fisher, R. Dhamija, and M.A. Hearst. Animated Exploration of Dynamic Graphs with Radial Layout. *InfoVis'01*. pp. 43-50 2001.

[EN 10] Bruls, M., K. Huizing, and J.J. van Wijk. Squarified TreeMaps. In *Proceedings of Joint Eurographics and IEEE TCVG Symp. on Visualization (TCVG 2000)*: IEEE Press. pp. 33-42, 2000.

[EN 44] Treemaps for Space-Constrained Visualization of Hierarchies. 1998. http://www.cs.umd.edu/hcil/treemap-history/

[EN 43] Sarkar, M. and M.H. Brown. Graphical Fisheye Views of Graphs. *CHI'92*. pp. 83-91, May 1992.

[EN 32] Leung, Y.K. and M.D. Apperley, A Review and Taxonomy of Distortion-Oriented Presentation Techniques. *ACM Transactions on Computer-Human Interaction*, 1994. **1**(2): p. 126-160.

[EN 2] Barnes, J. and P. Hut, A Hierarchical O(N Log N) Force Calculation Algorithm. *Nature*, 1986. **324**(4).

[EN 36] Myers, B.A., A New Model for Handling Input. *ACM Transactions on Information Systems*, 1990. **8**(3): p. 289-320.

[EN 25] Igarashi, T. and K. Hinckley. Speed-Dependent Automatic Zooming for Browsing Large Documents. *UIST'00*. pp. 139-148, 2000.

Anmerkungen

continued from previous page.

Also see Nm/Fragment 183 25 where the source is mentioned.

[181.] Nm/Fragment 190 03

Verschleierung

Untersuchte Arbeit: Seite: 190, Zeilen: 3-16	Quelle: Heer et al 2005 Seite(n): 5 (internet version), Zeilen: right column 31, 32-33, 34-36, 37-48, 51-54
Colour Maps. [...] These maps can be configured directly, or automatically generated by analyzing attribute values.	*Color Maps*. [...] These maps can be configured directly, [...] or automatically generated by analyzing attribute values.
Integrated Search. Prefuse also supports efficient keyword search in large data sets. This component builds a tree (Prefix tree) of requested data attributes, enabling searches that run in time proportional to the size of the query string. Search results matching a given query are then available for visualization as a FocusSet in the ItemRegistry's FocusManager.	*Integrated Search*. [...] the toolkit includes a FocusSet implementation to support efficient keyword search of large data sets. This component builds a trie (prefix tree) of requested data attributes, enabling searches that run in time proportional to the size of the query string. Search results matching a given query are then available for visualization as a FocusSet in the ItemRegistry's FocusManager.
Event Logging. Prefuse also provides facilities for logging. It is bundled with an event logger for monitoring and recording both user interfacing events and internal events. These Recorded logs can also be used to review or replay a session. Prefuse also has synchronized the event logger with the output of an eye-tracker, enabling playback sessions annotated with subjects' fixation points.	*Event Logging*. prefuse includes an event logger for monitoring and recording events. This includes both user interface events (mouse movement, focus selection) and internal system events (addition and deletion of items from the registry). [...] Recorded logs can be used to review or replay a session. We have even synchronized the event logger with the output of an eye-tracker, enabling us to playback sessions annotated with subjects' fixation points.

Farbig

Anmerkungen

continued from previous page

Also see Nm/Fragment 183 25 where the source is mentioned.

[182.] Nm/Fragment 190 17

Verschleierung

Untersuchte Arbeit: Seite: 190, Zeilen: 17-31	Quelle: Heer et al 2005 Seite(n): 9 (internet version), Zeilen: right column 41-54
In this Section we discussed Prefuse (which we have used a tool for visualization purpose of this study), a user interface toolkit for crafting interactive visualizations of structured and unstructured data. The Prefuse supports the design of 2D visualizations of any data consisting of discrete data entities, such as graphs, trees, scatter plots, collections, and timelines. The Prefuse implements existing theoretical models of information visualization to provide a flexible framework for simplifying application design and enabling reuse and composition of visualization and interaction techniques. In particular, Prefuse contributes scalable abstractions for filtering abstract data into visual content and using lists of composable actions to manipulate data in aggregate.	In this paper we have introduced prefuse, a user interface toolkit for crafting interactive visualizations of structured and unstructured data. prefuse supports the design of 2D visualizations of any data consisting of discrete data entities, such as graphs, trees, scatter plots, collections, and timelines. prefuse implements existing theoretical models of information visualization to provide a flexible framework for simplifying application design and enabling reuse and composition of visualization and interaction techniques. In particular, prefuse contributes scalable abstractions for filtering abstract data into visual content and using lists of composable actions to manipulate data in aggregate.
The prototype constructed in the research study using the Prefuse toolkit demonstrates the flexibility and performance of the Prefuse architecture.	Applications built with the toolkit demonstrate the flexibility and performance of the prefuse architecture.

Farbig

Anmerkungen

continued from above

[183.] Nm/Fragment 191 01

Verschleierung

Untersuchte Arbeit: Seite: 191, Zeilen: 1-6	Quelle: Heer et al 2005 Seite(n): 10 (internet version), Zeilen: left column 4-6, 13-15
[The Prefuse is] part of a larger move to systematize information visualization research and bring more interactivity into data analysis and exploration. The Prefuse is open-source software. The toolkit, source code, and both interactive and video demonstrations are available at http://Prefuse.sourceforge.net.	prefuse is part of a larger move to systematize information visualization research and bring more interactivity into data analysis and exploration. prefuse is open-source software. The toolkit, source code, and both interactive and video demonstrations are available at http://prefuse.sourceforge.net.

Farbig

Anmerkungen

continued from previous page;

this section concludes both the take-over and the original paper.

[184.] Nm/Fragment 191 10

Verschleierung

Untersuchte Arbeit: Seite: 191, Zeilen: 10-19	Quelle: Xu and Chen 2005a Seite(n): 104-105, Zeilen: p.104, right column 15-22 - p.105, left column 1-4
6.4 SUBGROUP DETECTION [FN 33] A terrorist network can often be partitioned into cells (subgroups) consisting of individuals who closely interact with each other. Given a network, traditional data mining techniques such as cluster analysis may be employed to detect underlying groupings that are not otherwise apparent in the data. Hierarchical clustering methods have been proposed to partition a network into subgroups (Wasserman, S., and Faust, K., 1994). Cliques whose members are fully or almost fully connected can also be detected based on clustering results. [FN 33] The most of the material presented in this Section is already published in (Memon N., Larsen Henrik Legind, 2006c)	[p. 104] **Subgroup detection** A criminal network can often be partitioned into subgroups consisting of individuals who closely interact with each other. Given a network, traditional data mining techniques such as cluster analysis may be employed to detect underlying groupings that are not otherwise apparent in [p. 105] the data. Hierarchical clustering methods have been proposed to partition a network into subgroups [EN 11]. Cliques whose members are fully or almost fully connected can also be detected based on clustering results. [EN 11] Wasserman, S., and Faust, K. *Social Network Analysis: Methods and Applications* (Cambridge: Cambridge University Press, 1994).

Farbig

Anmerkungen

Indeed: not only does this paragraph appear here in Nm's thesis but also in a number of Nm's papers, the earliest being a contribution to a conference in November 2005 and appearing here [7] (https://dspace.jaist.ac.jp/dspace/bitstream/10119/3913/1/20164.pdf) . Thus the formulation by Xu and Chen (2005a) presented here still predates any analogous text by Nm by at least several months. Nm's only contribution has been to change the object of research from "criminals" to "terrorists".

This furthermore begs the question if Nm's *iMiner* software prototype, which is at the heart of his thesis is far from Xu and Chen's *CrimeNet explorer*.

[185.] Nm/Fragment 191 20

Verschleierung

Untersuchte Arbeit: Seite: 191, Zeilen: 20-25	Quelle: Xu and Chen 2005a Seite(n): 106, Zeilen: right column 15-23
In this research and development study, we employed SNA techniques for terrorist intelligence analysis. The goal has been to provide law enforcement and intelligence agencies with third-generation network analysis techniques that not only produce graphical representations of terrorist networks but also provide structural analysis functionality to facilitate terrorist investigations.	Several data mining projects in the COPLINK research have begun to employ these SNA techniques for criminal network analysis. The goal has been to provide law enforcement and intelligence agencies with third-generation network analysis techniques that not only produce graphical representations of criminal networks but also provide structural analysis functionality to facilitate crime investigations.

Farbig

Anmerkungen

continues the take-over from Xu and Chen (2005a) (but from a different page than before)

[186.] Nm/Fragment 192 01

Verschleierung

Untersuchte Arbeit: Seite: 192, Zeilen: 1-12	Quelle: Smith and King 2002 Seite(n): 5 (internet version), Zeilen: left column 18-23 , right column 1-12
The iMiner is an experimental system, which provides facilities for retrieval of information and its presentation in graph form. A number of facilities that enable small subgraphs to be retrieved and added to the browsing canvas are also provided. In the current implementation we have provided four such facilities that are described in next section. **6.4.1 The Subgraph Retrieval Facilities** An analyst begins to construct a view by placing one or more objects on the browsing canvas, either by selecting from the list of those stored, or by retrieving objects according to their attribute values. The user may then begin to use the facilities that we now describe using the example of the database shown in Figure. 6.3.	The *Exploratory Database View Constructor (EDVC)* is an experimental system, which provides facilities for the incremental exploratory retrieval of information and its presentation in graph form as described in section 2 above. A number of facilities that enable small sub-graphs to be retrieved and added to the browsing canvas [FN 13] are also provided. In the current implementation we have provided seven such facilities that are described in the next section. **5.2 The sub-graph retrieval facilities** **5.2.1 Introduction** The user begins to construct a view by placing one or more objects on the browsing canvas, either by selecting from a list of those stored, or by retrieving objects according to their attribute values [FN 14]. The user may then begin to use the facilities that we now describe using the example database shown in figure 5.1 [FN 15]. --- [FN 13] We use the term “browsing canvas” throughout this section to refer to the display area on which the database view or chart is constructed. [FN 14] Objects are retrieved in this manner by specifying conditions that the attribute values of the objects retrieved must satisfy. These conditions are specified in an attribute condition grid similar to that used in QBE [ZLOO75]. [FN 15] The criminal intelligence database depicted in figure 5.1 and the examples presented throughout this section are based upon those presented in [AYRE95].

Farbig

Anmerkungen

It has already been officially noted in 2009 (see [8] (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5066528)) that Nm has taken parts of this source for yet another of his papers with "insufficient attribution (including appropriate references to the original author(s) and/or paper titles) and without permission".

Here the source is not given, either.

[187.] Nm/Fragment 193 01

Verschleierung

Untersuchte Arbeit: **Seite: 193, Zeilen: 1-12**	**Quelle: Smith and King 2002** **Seite(n): 6 (internet version), Zeilen: left column 12-26** Farbig
6.4.1.1 Retrieving all objects that are directly or indirectly connected to a specified object	**5.2.3 Retrieving all objects that are directly or indirectly connected to a specified object**
This facility may be used to retrieve and display all objects stored in the database that are connected an object already displayed on the browsing canvas by a path in the database of an arbitrary length, the associated connecting paths also being displayed. A user may specify the maximum length of a path from the object and the type of links that a connecting path may include.	The *vicinity* facility may be used to retrieve and display all objects stored in the database that are connected to an object already displayed on the browsing canvas by a path in the database of an arbitrary length, the associated connecting paths also being displayed. The user may specify the maximum length of a path from the object and the type of links that connecting paths may include.
For example, if an object representing Saeen was placed on the browsing canvas and this facility was used to display all objects connected to Saeen by a path of length two or less then the objects and links shown in Figure 6.4 would be displayed.	For example, if the object representing Sandra was placed on the browsing canvas and the vicinity facility was used to display all objects connected to Sandra by a path of length two or less then the objects and links shown in figure 5.2 would be displayed.

Anmerkungen

continued from previous page

[188.] Nm/Fragment 194 01

Verschleierung

Untersuchte Arbeit: **Seite: 194, Zeilen: 1-7**	**Quelle: Smith and King 2002** **Seite(n): 6 (internet version), Zeilen: right column 7-16** Farbig
6.4.1.2 Finding paths that connect two specified objects	**5.2.4 Finding paths that connect two specified objects**
If *Saeen* was to be charged with participating in a bombing plot and the police suspected that *Mars* was also involved, the investigative officer(s) would be likely to want to know if, and how, *Mars* and *Saeen* are connected. Paths in the database connecting two specified entities already on the browsing canvas may be displayed using all path facility as shown in Figure 6.5.	If Sandra was to be charged with participating in an armed robbery and the police suspected that Mary was also involved, the investigating officer(s) would be likely to want to know if, and how, Mary and Sandra are connected. Paths in the database connecting two specified objects already on the browsing canvas may be displayed using either the path facility, or the structured path facility.
[Text accompanying Figure 6.5]	[Text accompanying Figure 5.3]
Figure 6.5. The using all path facility to display all those paths in the database that is displayed in Fig. 2. that connect the objects representing Saeen and Mars.	Figure 5.3: The result of using the path facility to display all those paths in the database that is displayed in figure 5.1 of length four or less that connect the objects representing Sandra and Mary.

Anmerkungen

continued from previous page.

Note how Nm adapts the text to make it suitable for the terrorithm theme of the thesis: "Mary" becomes "Mars", "Sandra" becomes "Saeen" and an "armed robbery" becomes a "bombing plot".

[189.] Nm/Fragment 195 02

Verschleierung

Untersuchte Arbeit: Seite: 195, Zeilen: 2-12	Quelle: Smith and King 2002 Seite(n): 7 (internet version), Zeilen: left column 10-19, 30-37
6.4.1.3 Finding connections between groups of objects	**5.2.5 Finding connections between groups of objects**
Consider the following witness statement, "I saw *Alam* and *Memon* in a car with two other men. If *Alam* and *Memon* were two suspects in a terrorist plot then the police would like to identify the two other men. Support for finding connections between groups of objects is provided by this facility.	Consider the following witness statement, "I saw Alan and Mike drinking in the King George public house with two other men. They left in a van with Kelly Building Contractors written on the side". If Alan and Mike were two suspects in an armed robbery then the police would want to identify the two other men. Support for finding connections between groups of objects is provided through the *centre* facility.
Consider the witness statement above, using this facility to retrieve objects that are instances of the person object class and connected to the objects *Victoria Garage*, *Saeen*, *London Gym*, and *Donald* as shown in Figure 6.6. Thus, *Saeen* and *Donald* are identified as possible companions of *Alam* and *Memon*.	[...] Consider the witness statement above. Using the centre facility to retrieve objects that are instances of the person object class and connected to the objects Mike, Alan, the King George, and the Kelly Building firm by a path of length three or less would result in the objects and links shown in figure 5.5. Thus Joe, Richard and Ronald are identified as possible drinking companions, [...]

Farbig

Anmerkungen

continued from previous page

adapted to "terrorism research" and using a slightly changed example, otherwise nearly identical

[190.] Nm/Fragment 198 03

Verschleierung

Untersuchte Arbeit: Seite: 198, Zeilen: 3-18	Quelle: Xu and Chen 2005b Seite(n): 201, Zeilen: 5-15
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 organizations data. To help law enforcement and intelligence agencies discover terrorist network knowledge efficiently and effectively, in this research we propose a framework for automated network analysis, visualization and destabilization. Based upon this framework, this project developed a system called iMiner that incorporates several advanced techniques: subgroups detection approach, discovering efficiency of a network, social network analysis methods, destabilizing strategies for terrorist networks including detection of hidden hierarchy.	Knowledge about the structure and organization of criminal networks is important for both crime investigation and the development of effective strategies to prevent crimes. However, except for network visualization, criminal network analysis remains primarily a manual process. Existing tools do not provide advanced structural analysis techniques that allow extraction of network knowledge from large volumes of criminal-justice data. To help law enforcement and intelligence agencies discover criminal network knowledge efficiently and effectively, in this research we proposed a framework for automated network analysis and visualization. The framework included four stages: network creation, network partition, structural analysis, and network visualization. Based upon it, we have developed a system called CrimeNet Explorer that incorporates several advanced techniques: a concept space approach, hierarchical clustering, social network analysis methods, and multidimensional scaling.

Farbig

Anmerkungen

This is just the introduction from the major paper of Xu and Chen (2005b), in which they present their "CrimeNet Explorer" system, slightly rewritten to fit terrorist networks instead of criminal networks. The source is not named here.

[191.] Nm/Fragment 199 10

Verschleierung

Untersuchte Arbeit: Seite: 199, Zeilen: 10-15	Quelle: Perer_Shneiderman_2006 Seite(n): 693, Zeilen: right column
This chapter presents Investigative Data Mining Toolkit: iMiner, which is believed more than just another terrorist social network analysis tool because it balances systematic and flexible exploration. To help users systematically examine measures, iMiner applies new mathematical models and practical algorithms for analysis and destabilizing terrorist networks.	We present *SocialAction*, which we believe is more than just a YASNAT ("yet another social network analysis tool") because it balances systematic and flexible exploration. To help users systematically examine measures, *SocialAction* applies attribute ranking and coordinated views to identify extreme-valued nodes (Section 3).

Farbig

Anmerkungen

No source given. One gets the impression that iMiner possibly is a YASNAT.

[192.] Nm/Fragment 199 27

Verschleierung

Untersuchte Arbeit: Seite: 199, Zeilen: 27-28	Quelle: Xu and Chen 2005a Seite(n): 106, Zeilen: right column 32-36
The first stage of network analysis development is to automatically identify the [strongest association paths, or geodesics, between two or more network members.]	The first stage of our network analysis development was intended to automatically identify the strongest association paths, or geodesics, between two or more network members using shortest-path algorithms.

Farbig

Anmerkungen

reference is never named

[193.] Nm/Fragment 200 01

Verschleierung

Untersuchte Arbeit: Seite: 200, Zeilen: 1-4	Quelle: Xu and Chen 2005a Seite(n): 106, Zeilen: right column 32-39
[The first stage of network analysis development is to automatically identify the] strongest association paths, or geodesics, between two or more network members. In practice, such a task often entails intelligence officials manually exploring links and trying to find association paths that might be useful for generating investigative leads.	The first stage of our network analysis development was intended to automatically identify the strongest association paths, or geodesics, between two or more network members using shortest-path algorithms. In practice, such a task often entails crime analysts to manually explore links and try to find association paths that might be useful for generating investigative leads.

Farbig

Anmerkungen

no reference given

[194.] Nm/Fragment 202 12

Verschleierung

Untersuchte Arbeit: Seite: 202, Zeilen: 12-21	Quelle: Tsvetovat et al. 2005 Seite(n): 2, Zeilen: 13ff	Farbig
In the aftermath of the September 11th attacks, it was noted that comprehensible information sources were not available to the researchers (Sageman 2004). Information was either available in a disconnected form, not allowing for comparison studies across events, groups or tactics, or made available in written articles – which are not readily suitable for quantitative analysis of terrorist networks. Data collected by law enforcement agencies, while potentially better organized, are largely not available to the research community due to restrictions in distribution of sensitive information.	In the aftermath of the September 11th attacks, it was noted that coherent information sources on terrorism and terrorist groups were not available to researchers[10]. Information was either available in fragmentary form, not allowing comparison studies across incidents, groups or tactics, or made available in written articles - which are not readily suitable for quantitative analysis of terrorist networks. Data collected by intelligence and law-enforcement agencies, while potentially better organized, is largely not available to the research community due to restrictions in distribution of sensitive information.	

[10] Le Gruenwald, Gary McNutt, and Adrien Mercier. Using an ontology to improve search in a terrorism database system. Proceedings of the 14th International Workshop on Database and Expert System Applications (DEXA'03), 2003.

Anmerkungen

The source is not mentioned anywhere in the thesis

[195.] Nm/Fragment 205 21

Verschleierung

Untersuchte Arbeit: Seite: 205, Zeilen: 21-23	Quelle: Zhao et al 2006 Seite(n): 2, Zeilen: left column 40-42	Farbig
The iMiner knowledge base (see Figure 7.5) consists of various types of entities. Here is an incomplete list of the different entity types:	The PIT knowledge base consists of various types of entities. Here is an incomplete list of the different entity types:	

Anmerkungen

This is just the start of the nearly word-for-word copy of descriptions and names for entities and relation types of a knowledge base for "counter-terrorism research". This begs the question if Nm's iMiner knowledge base - which is supposed to be the scientific core of his thesis - is as original as it should be or if it is also just a copy - a copy of the PIT knowledge base which is described in the unnamed source.

[196.] Nm/Fragment 206 01

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 206, Zeilen: 1-21	Quelle: Zhao et al 2006 Seite(n): 2, Zeilen: left column 43-49, right column 1, 13-30
• Terrorist organizations such as Al Qaeda	• **Terrorist organizations** such as Hamas, Hizballah, Liberation Tigers of Tamil Eelam (LTTE), etc.
• Terrorists such as Osama Bin Ladin, Ramzi Yousef, etc.	• **Terrorists** such as Osama bin Ladin, Ramzi Yousef, etc.
• Terrorist facilities such as Darunta Training Camp, Khalden Training Camp, etc.	• **Terrorist facilities** such as Darunta Training Camp, Khalden Training Camp, etc.
• Terrorist events/attacks such as 9/11, WTC terrorist attack 2003, etc.	• **Terrorist events/attacks** such as African embassy bombings of 1998, Madrid Bombings of 2004, etc.
The dataset also contains various types of relations connecting instances of different entity types. Here is a partial list of the various relation types:	[...]
• memberOf: instances of terrorist can be affiliated with various instances of terrorist organization.	The dataset also contains various types of relations connecting instances of different entity types. Here is a partial list of the various relation types:
• facilityOwner: instances of terrorist facility are usually run by instances of terrorist organizations.	• **memberOf**: instances of **terrorist** can be affiliated with various instances of **terrorist organization**.
• facilityMember: instances of terrorist are linked to various instances of terrorist facilities if the terrorist instance attended/spent some time at the facility.	• **facilityOwner**: instances of **terrorist facility** are usually run by instances of **terrorist organizations**.
• claimResponsibility: instances of terrorist organization are linked to the instances of terror attacks they claim responsibility for.	• **facilityMember**: instances of **terrorist** are linked to various instances of **terrorist facilities** if the **terrorist** instance attended/spent some time at the facility.
• participatedIn: instances of terrorist that may have participated in instances of terror attacks.	• **claimResponsibility**: instances of **terrorist organization** are linked to the instances of **terror attacks** they claim responsibility for.
	• **participate**: instances of **terrorist** may participate in instances of **terror attacks**.

Anmerkungen

continues the verbatim take-over of the description of another research group's counter-terrorism knowledge base;

Mark also the transcription "Bin Ladin" which corresponds to the one given in the source, but which is used nowhere else in Nm's thesis (Usually Nm writes "Bin Laden").

[197.] Nm/Fragment 206 26

KomplettPlagiat

Untersuchte Arbeit: Seite: 206, Zeilen: 26-28	Quelle: Jensen et al 2003 Seite(n): 381, Zeilen: left column 6-12
The analysis of relational data is a rapidly growing area within the larger research community interested in machine learning, knowledge discovery, and data mining. Several workshops [(Dzeroski, S., De Raedt, L., and Wrobel, S. 2002; Getoor, L., and Jensen, D. 2000; Jensen, D. and Goldberg, H. 1998) have focused on this particular topic, and another DARPA research program — Evidence Extraction and Link Discovery (EELD) —focuses on extracting, representing, reasoning with, and learning from relational data.]	Analysis of relational data is a rapidly growing area within the larger research community interested in machine learning, knowledge discovery, and data mining. Several recent workshops [EN 3, EN 6, EN 8] have focused on this precise topic, and another DARPA research program — Evidence Extraction and Link Discovery (EELD) —focuses on extracting, representing, reasoning with, and learning from relational data. [FN 5] --- [EN 3] Dzeroski, S., De Raedt, L., and Wrobel, S. (Eds). Papers of the Workshop on Multi-Relational Data Mining. The Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM Press, 2002. [EN 6] Getoor, L., and Jensen, D. (Eds). Learning Statistical Models from Relational Data: Papers from the AAAI 2000 Workshop, AAAI Press, Menlo Park CA, 2000. [EN 8] Jensen, D. and Goldberg, H. Artificial Intelligence and Link Analysis: Papers from the 1998 AAAI Fall Symposium., AAAI Press, Menlo Park CA, 1998.

Farbig

Anmerkungen

Verbatim with the references as in the source, which is not referenced, although it represents another workshop of those described.

[198.] Nm/Fragment 207 01

KomplettPlagiat

Untersuchte Arbeit: Seite: 207, Zeilen: 1-6	Quelle: Jensen et al 2003 Seite(n): 381, Zeilen: left column 6-12
[The analysis of relational data is a rapidly growing area within the larger research community interested in machine learning, knowledge discovery, and data mining. Several workshops] (Dzeroski, S., De Raedt, L., and Wrobel, S. 2002; Getoor, L., and Jensen, D. 2000; Jensen, D. and Goldberg, H. 1998) have focused on this particular topic, and another DARPA research program — Evidence Extraction and Link Discovery (EELD) —focuses on extracting, representing, reasoning with, and learning from relational data.	Analysis of relational data is a rapidly growing area within the larger research community interested in machine learning, knowledge discovery, and data mining. Several recent workshops [EN 3, EN 6, EN 8] have focused on this precise topic, and another DARPA research program — Evidence Extraction and Link Discovery (EELD) —focuses on extracting, representing, reasoning with, and learning from relational data. [FN 5] --- [EN 3] Dzeroski, S., De Raedt, L., and Wrobel, S. (Eds). Papers of the Workshop on Multi-Relational Data Mining. The Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM Press, 2002. [EN 6] Getoor, L., and Jensen, D. (Eds). Learning Statistical Models from Relational Data: Papers from the AAAI 2000 Workshop, AAAI Press, Menlo Park CA, 2000. [EN 8] Jensen, D. and Goldberg, H. Artificial Intelligence and Link Analysis: Papers from the 1998 AAAI Fall Symposium., AAAI Press, Menlo Park CA, 1998.

Farbig

Anmerkungen

continued from previous page

[199.] Nm/Fragment 207 12

KomplettPlagiat

Untersuchte Arbeit: Seite: 207, Zeilen: 12-18, 20, 21-22	Quelle: Frost 1982 Seite(n): 358, Zeilen: left column 30-37, 38-40
The binary–relational view regards the universe as consisting of entities with binary–relationships between them. An entity is anything which is of interest and can be identified. A binary–relationship is an association between two entities. The first entity in a relationship is called the subject and the second entity is called the object. A relationship is described by identifying the subject, the type of relationship, and object for example: Bin Laden is leader of Al Qaeda can be written as (Bin Laden. leaderOf .Al Qaeda). N–ary relationships such as Samad got bomb making training from Zarqawi may be reduced to a set of binary–relationships by the explicit naming of the implied entity. For example: training # 1. trainee .Samad training #1. trainer .Zarqawi training #1. got training of .bomb making	The binary-relational view regards the universe as consisting of entities with binary-relationships between them. An entity is any 'thing' which is of interest and can be identified. A binary-relationship is an association between two entities. The first entity in a relationship is called the subject and the second entity is called the object. A relationship is described by identifying the subject, the type of relationship, and the object. For example: IBM • employs • John N—ary relationships such as 'John bought the car from Smiths' may be reduced to a set of binary-relationships by the explicit naming of the implied entity. For example: sale # 1 . buyer . John sale # 1 . seller . Smiths sale # 1 . item sold . car

Farbig

Anmerkungen

Identical, except for the examples (and one article). Not marked as a citation. The source is mentioned some lines below but there it is obviously supposed to refer to the sentences that follow.

[200.] Nm/Fragment 208 01

BauernOpfer

Untersuchte Arbeit: Seite: 208, Zeilen: 1-10	Quelle: Frost 1982 Seite(n): 359, Zeilen: right column 20-28
* Simple interface between a binary relational storage structure and other modules of a database management system consists of three procedures: ▪ insert (triple); (ii) delete (partial specification of triple); (iii) retrieve partial specification of triple) ▪ Retrieval requests such as “list of all that terrorists met at Malaysia before 9/11” are met by issuing simple retrieval call (terrorist. met at Malaysia before 9/11. ?) which delivers only that data which has been requested.	**Simple interface with other modules** Interface between a binary-relational storage structure and other modules of a database management system consists of three procedures: (i) insert (triple); (ii) delete (partial specification of triple); (iii) retrieve (partial specification of triple). Retrieval requests such as 'list all employees of IBM' are met by issuing a simple retrieval call (IBM. employs. ?) which delivers only that data which has been requested

Farbig

Anmerkungen

The source is named on the previous page. Nevertheless it is not to be expected that Nm, follows it word-for-word, given there are no quotation marks.

[201.] Nm/Fragment 208 11

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 208, Zeilen: 11-15, 17-18, 24-28	Quelle: Frost 1982 Seite(n): 360-361, Zeilen: p.360, right column 51-56 & p.361, left column, 1-2.9-14
It is to be noted that multi-attribute retrieval may be inefficient. The use of binary relational structure for multi-attribute retrieval might not be the most efficient method (irrespective of the way in which the structure is implemented. To illustrate this, consider the example: “retrieve (the names of) all young (25 years old) married terrorists involved in 9/11 attacks who attended flight schools and got terrorist training in Afghanistan”. Using binary-relational structure, one could issue the retrievals: (? .marital status. Married) (? .age. 25) (? .involved in. 9/11 terrorist attacks) (? .attended. flight schools) (? .got terrorist training. Afghanistan) and merge the resultant sets to obtain the required data. This is probably much faster than having to do a sequential search through the whole database, which would be necessary if the database were held as a file of records (name, age, marital status, etc.) ordered on name.	[p. 360] **Multi-attribute retrieval may be inefficient** Use of a binary-relational structure for multi-attribute retrieval might not be the most efficient method (irrespective of the way in which the structure is implemented). To illustrate this, consider the example given by Martin[EN 12]: 'retrieve (the names of) all 18 year old unemployed actresses with experience in movie-acting, [p. 361] and talents for singing and sky-diving'. Using a binary relational structure, one could issue the retrievals: (?. aged. 18) (?. job-status, unemployed) (?. profession, actress) (?. experience, movie-acting) (?. talent, singing) (?. talent, sky-diving) and merge the resultant sets to obtain the required data. This is probably much faster than having to do a sequential search through the whole database, which would be necessary if the database were held as a file of records (name, age, job-status, profession, experience, talents) ordered on name.

Anmerkungen

Continues the copying from Frost (1982). The example given seems to be one of Nm's own making.

[202.] Nm/Fragment 214 02

Verschleierung

Farbig

Untersuchte Arbeit: Seite: 214, Zeilen: 2-7	Quelle: TrackingTheThreat.com 2006a Seite(n): 1 (internet version), Zeilen: 2-5
The http://www.trackingthethreat.com/ is a knowledge base of open source information about the Al Qaeda terrorist network, developed as a research project of the FMS Advanced Systems Group. The main goal of this project is to apply new technologies and software engineering approaches to open source intelligence while providing researchers and analysts with information about Al Qaeda.	TrackingTheThreat.com is database of open source information about the Al Qaeda terrorist network, developed as a research project of the FMS Advanced Systems Group. Our goal is to apply new technologies and software engineering approaches to open source intelligence while providing researchers and analysts with information about Al Qaeda.

Anmerkungen

A near literal copy of TrackingTheThreat.com self-description; nothing is marked as a citation.

[203.] Nm/Fragment 214 07

KomplettPlagiat

Untersuchte Arbeit: Seite: 214, Zeilen: 7-14	Quelle: TrackingTheThreat.com 2006 Seite(n): 1 (internet version), Zeilen: 53-57
This site contains information collected from thousands of open source reports, documents, news stories, and other places which are deemed appropriate. It is presented in a concise and organized fashion as a demonstration of some of the capabilities of Sentinel TMS. The group have attempted to assign some degree of credibility to its accuracy, no representation is made or implied that all data contained herein is completely reliable.	This site contains information collected from thousands of open source reports, documents, news stories, and other places which are deemed worthy of note. It is presented here in a concise and organized fashion as a demonstration of some of the capabilities of Sentinel TMS. While we have attempted to assign some degree of credibility to its accuracy, no representation is made or implied that all data contained herein is completely reliable.

Farbig

Anmerkungen

A barely concealed copy of the original text.

[204.] Nm/Fragment 214 15

Verschleierung

Untersuchte Arbeit: Seite: 214, Zeilen: 15-24	Quelle: TrackingTheThreat.com 2006 Seite(n): 1 (internet version), Zeilen: 2-10
This knowledge base represents the original open-source knowledge base on Al Qaeda. It contains data in the form of:	TrackingTheThreat.com is database of open-source information about the Al Qaeda terrorist network. It contains data in the form of:
Entities: Discrete data elements that comprise people, places, organizations, events, etc.	• **Entities**: Discrete data elements that comprise people, places, organizations, events, etc.
Relationships: Information about the personal, organizational, transactional, and historical connections between entities.	• **Relationships**: Information about the personal, organizational, transactional, and historical connections between entities.
Metadata: Additional information about entities and relationships that help form a more complete picture.	• **Metadata**: Additional information about entities and relationships that help form a more complete picture.
Notes and Documents: Unstructured text that provides background information on entities, relationships, and metadata.	• **Notes and Documents**: Unstructured text that provides background information on entities, relationships, and metadata.

Farbig

Anmerkungen

an almost literal copy, not marked as a citation

[205.] Nm/Fragment 215 01

Verschleierung

Untersuchte Arbeit: Seite: 215, Zeilen: 1-4	Quelle: Dugan_etal_2006 Seite(n): 409, Zeilen: 29-32
[The weakness of the] knowledge base includes potential media bias and misinformation, lack of information beyond incident specific details alone, and missing data which was not available in the media. We review some of these strength and weaknesses in the next section of this article.	Weaknesses of the database include potential media bias and misinformation, lack of information beyond incident specific details alone, and missing data from a set of cards that were lost during an office move of PGIS. We review some of these strengths and weaknesses in the next section of this report.

Farbig

Anmerkungen

The source is not mentioned anywhere in the thesis

[206.] Nm/Fragment 215 11

Verschleierung

Untersuchte Arbeit: **Seite: 215, Zeilen: 11-31**	**Quelle: Malin_etal_2005** **Seite(n): 119, 120, Zeilen: 30ff; 1ff**

Farbig

Investigative data mining is increasingly performed on networks constructed from personal name relationships extracted from text-based documents. In such networks, a node corresponds to a particular name and an edge specifies the relationship between two names. Before such a network can be analyzed for centrality, grouping, or intelligence gathering purposes, the correctness of the network must be maximized. Specifically, it must be decided when two pieces of data correspond to the same entity or not. Failure to ensure correctness can result in the inability to discover certain relationships or the cause of learning false knowledge.

Names are not unique identifiers for specific entities and, as a result, there exists many confounders to the construction of correct networks. Firstly, the data may consist of typographical error. In this case, the name “Nasrullah” may be accidentally represented as “Nasarullah” or “Nasurullah”. There exists a number of string comparator metrics to account for typographical errors, many of which are in practice.

However, even when names are free of typographical errors, there are additional confounders to data correctness. For example, there may occur name variation, where multiple names correctly reference the same entity or same name correctly references multiple entities i.e., there can exist name ambiguity.

Link analysis is increasingly performed on networks constructed from personal name relationships extracted from text-based documents

[...] [P. 120] [...]

In such networks, a vertex corresponds to a particular name and an edge specifies the relationship between two names. Before such a network can be analyzed for centrality, grouping, or intelligence gathering purposes, the correctness of the network must be maximized. Specifically, it must be decided when two pieces of data correspond to the same entity or not. Failure to ensure correctness can result in the inability to discover certain relationships or cause the learning of false knowledge.

Names are not unique identifiers for specific entities and, as a result, there exist many confounders to the construction of correct networks. Firstly, the data may consist of typographical error. In this case, the name “John” may be accidentally represented as “Jon” or “Jhon”. There exist a number of string comparator metrics (Winkler, 1995; Cohen et al., 2003;Wei, 2004) to account for typographical errors, many of which are in practice by various federal statistical agencies, such as the U.S. Census Bureau. However, even when names are devoid of typographical errors, there are additional confounders to data correctness. For instance, there can exist name variation, where multiple names correctly reference the same entity. Or, more pertinent to our research, there can exist name ambiguity, such that the same name correctly references multiple entities.

Anmerkungen

The source is not mentioned anywhere in the thesis.

[207.] Nm/Fragment 216 05

Verschleierung

Untersuchte Arbeit: Seite: 216, Zeilen: 5-30	**Quelle: Dugan_etal_2006 Seite(n): 410-411, Zeilen: p 410: 39ff; p 411: 1ff**

Farbig

7.4.2 Weaknesses of Open Source Knowledge bases

As discussed above, the original knowledge base has some important strength; this study also recognizes that it also has significant weaknesses that need to be understood when drawing conclusions from data. Two types of weaknesses are especially important. First, all major open source databases rely on data culled from news resources; they are likely biased toward the most newsworthy forms of terrorism (Fowler, W. W., 1981).

Although the original knowledge base under discussion, includes events that were prevented by authorities (for example the Bojinka terrorists plan), it is certain that some potential terrorist attacks never came to the attention of the media and are thus excluded. A related issue is that the original knowledge base includes incidents covered by media where criminals/ terrorists remain undisclosed. Without information concerning a criminal/ terrorist it may be difficult to accurately classify an incident as terrorism. Also, various media accounts of similar terrorist incidents may contain conflicting information. Without measures of reliability in news reporting, it is difficult for researchers to distinguish, which source supplies the most perfect account.

The second issue is that the original knowledge base lacks information on other important issues associated with each terrorism incident. Open source databases also lack information on the psychological characteristics, recruitment, and careers of members of terrorist movements. A lack of data on terrorist networks is mainly explained by their covert nature.

4.2 Weaknesses of Open Source Terrorism Databases

But while the PGIS data has some important strengths, we also recognize that it also has important weaknesses that need to be understood when drawing conclusions from the data. Three types of weaknesses are especially important. First, all the major open source terrorism databases (ITERATE, MIPT-RAND and PGIS) rely on data culled from news sources, thus they are likely biased toward the most newsworthy forms of terrorism [6]. Although the PGIS database includes events that were prevented by [page 411] authorities, it is certain that some potential terrorist attacks never came to the attention of the media and are thus excluded. A related issue is that the PGIS database includes incidents covered by the media where the perpetrator remains unidentified. Without information concerning the perpetrator it may be difficult to accurately classify the incident as terrorism, since the definition relies on the motive of the attacker. Finally, various media accounts of similar terrorist incidents may contain conflicting information. Without measures of reliability in news reporting, it is difficult for researchers to discern which source supplies the most accurate account.

The second issue is that the dataset lacks information on other important issues associated with each terrorism incident. Open source databases, including the one created by PGIS also lack information on the "psychological characteristics, recruitment, and careers of members of terrorist movements" [9:28]. [...] Of course, the lack of data on terrorist groups is mainly explained by their clandestine nature.

---

[6]. Fowler, W. W. (1981). [...]

Anmerkungen

The text has been copied with only slight adaptations, the source is not mentioned in the thesis anywhere

[208.] Nm/Fragment 219 04

Verschleierung

Untersuchte Arbeit: Seite: 219, Zeilen: 4-8, 10-23, 24-26	Quelle: Balasundaram et al 2006 Seite(n): 1, 2, Zeilen: 1:18-21; 2:4-11.35-39 Farbig
In the wake of the information revolution, the interest in studying the network structure of organizations, in particular criminal in nature, has increased manifold. Social network concepts, regardless of their flexibility, have come to the forefront especially for these applications. This chapter introduces and studies cohesion analysis of terrorist networks. *Cohesion analysis* is often used to explain and develop sociological theories. Members of a cohesive subgroup tend to share information, have homogeneity of thought, identity, beliefs, behaviour, even food habits and illnesses (Wasserman, S., Faust, K., 1994). Social cohesion is also believed to influence emergence of consensus among group members. Examples of cohesive subgroups include religious sects, terrorist groups, criminal gangs/ organized criminals, military teams, and tribal clusters, etc. Some direct application areas of social networks include studying terrorist networks (Sageman, M., 2004; Berry, N. *et al*., 2004), as mentioned earlier chapters a special application of criminal network analysis. It is anticipated to study organized crimes for example, terrorism, drug trafficking and money laundering, (McAndrew, D.,1999:; Chen, H. *et al*, 2004)), identity theft, credit card crime, child pornography, human smuggling. It is worthy to mention that SNA concepts provide suitable data mining tools for this purpose (Davis, R.H, 1981).	In the wake of the information revolution, the interest in studying the network structure of organizations, in particular criminal in nature, has increased manifold. Social network concepts, despite their versatility, have come to the forefront especially for these applications. [...] [Page 2] *Social cohesion* is often used to explain and develop sociological theories. Members of a cohesive subgroup tend to share information, have homogeneity of thought, identity, beliefs, behavior, even food habits and illnesses [52]. Social cohesion is also believed to influence emergence of consensus among group members. Examples of cohesive subgroups include religious cults, terrorist cells, criminal gangs, military platoons, sports teams and conferences, work groups etc. [...] Some direct application areas of social networks include studying terrorist networks [43,9], which is essentially a special application of criminal network analysis that is intended to study organized crimes such as terrorism, drug trafficking and money laundering [36,21]. Concepts of social network analysis provide suitable data mining tools for this purpose [17]. --- [9]. Berry, N., Ko, T., Moy, T., Smrcka, J., Turnley, J., Wu, B.:[...] (2004). [...] [17]. Chen, H., Chung, W., Xu, J.J., Wang, G., Qin, Y., Chau, M.: [...] (2004) [21]. Davis, R.H.:[...] (1981) [36]. McAndrew, D.: [...] (1999) [43]. Sageman, M.: [...] (2004) [52]. Wasserman, S., Faust, K.: [...] (1994)

Anmerkungen

The source is not given. The text is copied including all literature references. Only minor adjustments have been made.

[209.] Nm/Fragment 219 27

Verschleierung

Untersuchte Arbeit: Seite: 219, Zeilen: 27-28	Quelle: Stokman_2004 Seite(n): 1, Zeilen: 1-3 Farbig
Social network analysis in general studies behaviour of the individuals at the micro level, the pattern of relationships (network [structure) at the macro level, and the interactions between the two.]	Social network analysis [FN 1] studies the behavior of the individual [FN 2] at the micro level, the pattern of relationships (network structure) at the macro level, and the interactions between the two.

Anmerkungen

To be continued on the next page. The source is not mentioned in the thesis at all.

[210.] Nm/Fragment 220 01

Verschleierung

Untersuchte Arbeit: Seite: 220, Zeilen: 1-14	Quelle: Stokman_2004 Seite(n): 1, Zeilen: 1-12
[Social network analysis in general studies behaviour of the individuals at the micro level, the pattern of relationships (network] structure) at the macro level, and the interactions between the two. The analysis of the communication structures that is comprised in SNA study is known as an important element in the analysis of the micro-macro link, the way in which individual behaviour and social phenomena are linked with one another. In this sense, social networks can assist the analysts both the root cause and the result of the behaviour of an individual. It is fact that social networks study provides and bound chances of individual selections in the mean-time time individuals initiate, build, continue, and break up links and by doing so define the universal structure of a network. However, network structure is seldom constructed by its individuals. It is known as the 'unintended' effect of the actions of the individual and can as be called a "spontaneous order".	Social network analysis [FN 1] studies the behavior of the individual [FN 2] at the micro level, the pattern of relationships (network structure) at the macro level, and the interactions between the two. The analysis of the interaction structures that is involved in social network analysis is an important element in the analysis of the macro-micro-macro link, the way in which individual behavior and collective phenomena are connected with one another. In this perspective, social networks are both the cause of and the result of individual behavior. Social networks provide and limit opportunities of individual choices, whereas at the same time individuals initiate, construct, maintain, and break up relationships and by so doing determine the global structure of the network. However, individuals seldom consciously construct network structures beyond their own relationships. The overall network structures are often the 'unintended' effect of individual actions and can as such be called a "spontaneous order" (see e.g. Hayek 1973).

Farbig

Anmerkungen

No reference given. The content is identical, but formulations have been somewhat adapted.

[211.] Nm/Fragment 220 14

Verschleierung

Untersuchte Arbeit: Seite: 220, Zeilen: 14-29	Quelle: Aviv et al 2003 Seite(n): 4, Zeilen: 15-21
SNA methods provide specific mathematical definitions of five groups of characteristics of the actors/ nodes and of the network itself (Bonacich, P., 1987; Burt, R. S., 1992): 1. cohesion, 2. equivalence (role-groups), 3. power of actors, 4. range of influence, and 5. brokerage These characteristics are expressed in terms of corresponding network structure parameters derived from the relations among actors. There is vast amount of material is available for the introduction to SNA which can be easily, for example, in (Scott, J., 2000; Hanneman, R. E., 2005; Wasserman, S., Faust, K., 1994). The insights that can be obtained from the various values of the network structures are elaborated in Burt (1990)	SNA methods provide precise mathematical definitions of five groups of characteristics of the actors and of the network itself [EN 18, EN 19]: cohesion, equivalence (role-groups), power of actors, range of influence, and brokerage. These characteristics are expressed in terms of corresponding *Network-Structure* parameters derived from the relations among the actors. An introduction to SNA can be found in Scott [20] and Hanneman [21]. For a comprehensive text, see Wasserman and Faust [22]. Burt [13] elaborates on the insights that can be obtained from the various values of the network structures. [EN 18] **Bonacich, P.**, Power and Centrality. *American Journal of Sociology* 92: 1170-1182 (1987). [EN 19] '*Burt, R. S.*, *Structural Holes*, Cambridge, MA: Harvard University Press, 1992.

Farbig

Anmerkungen

Looks like a bonafide overview on the subject done by Nm, but in fact Nm only copies what already could be found in Aviv (2003). No reference to Aviv given.

[212.] Nm/Fragment 221 23

Verschleierung

Untersuchte Arbeit: Seite: 221, Zeilen: 23-29	Quelle: Balasundaram et al 2006 Seite(n): 2, Zeilen: 11-15
It is reported that mathematically modeling a cohesive subgroup has been a subject of interest in social network analysis since many decades. As stated earlier, one of the earliest graph models used for studying cohesive subgroups was the *clique* model (Luce, R., Perry, A., 1949). A clique is a subgraph in which there is an edge between any two nodes. However, the clique approach has been criticized for its [restrictive nature.]	Modeling a cohesive subgroup mathematically has long been a subject of interest in social network analysis. One of the earliest graph models used for studying cohesive subgroups was the *clique* model [35]. A clique is a subgraph in which there is an edge between any two vertices. However, the clique approach has been criticized for its overly restrictive nature [...] [35]. Luce, R., Perry, A.: [...] (1949)

Farbig

Anmerkungen

To be continued on the next page: Nm/Fragment_222_01

[213.] Nm/Fragment 222 01

Verschleierung

Untersuchte Arbeit: Seite: 222, Zeilen: 1-25	Quelle: Balasundaram et al 2006 Seite(n): 2, Zeilen: 14-16, 18-24, 25-26, 28-34
[However, the clique approach has been criticized for its] restrictive nature. More details can be found in (Scott, J., 2000; Wasserman, S., Faust, K., 1994) and modeling disadvantages (Seidman, S.B., Foster, B.L., 1978; Freeman, L.C., 1992). It is important to note that clique models provide three important structural properties that are expected of a cohesive subgroup, namely: 1. *familiarity* (each node has many neighbours and only a few strangers in the group), 2. *reachability* (a low diameter, facilitating fast communication between the group members) and 3. *robustness* (high connectivity, making it difficult to destroy the group by removing members). As mentioned earlier, different models relax different aspects of a cohesive subgroup. In this context, Luce R. introduced a distance based model known as *n-clique* (Luce, R., 1950). This model was also studied along with a variant called *n-clan* by Mokken (1979). Some drawbacks are pointed out and the models are appropriately redefined in (Balasundaram, B., Butenko, S., Trukhanov, S., 2005). All these models highlight the need for high reachability inside a cohesive subgroup and have their own advantages and disadvantages as models of cohesiveness. The other variation is degree based model which is known as *k-plex* (Wasserman, S., Faust, K., 1994). This model relaxes familiarity within a cohesive subgroup and implicitly provides reachability and robustness.	However, the clique approach has been criticized for its overly restrictive nature [2,52] and modeling disadvantages [47,25]. [...] Clique models idealize three important structural properties that are expected of a cohesive subgroup, namely, *familiarity* (each vertex has many neighbors and only a few strangers in the group), *reachability* (a low diameter, facilitating fast communication between the group members) and *robustness* (high connectivity, making it difficult to destroy the group by removing members). Different models relax different aspects of a cohesive subgroup. [34] introduced a distance based model called *k-clique* [...]. These models were also studied along with a variant called *k-clan* by Mokken [38]. [...] These drawbacks are pointed out and the models are appropriately redefined in [7], as described in Section 2. All these models emphasize the need for high reachability inside a cohesive subgroup and have their own merits and demerits as models of cohesiveness. The focus of this paper is on a degree based model introduced in [47] and called *k-plex*. This model relaxes familiarity within a cohesive subgroup and implicitly provides reachability and robustness. [2]. Alba, R.: [...] (1973) [7]. Balasundaram, B., Butenko, S., Trukhanov, S.:[...] (2005) [25]. Freeman, L.C.: [...] (1992) [34]. Luce, R.:[...] (1950) [38]. Mokken, R.: [...] (1979) [47]. Seidman, S.B., Foster, B.L.: [...] (1978) [52]. Wasserman, S., Faust, K.: [...] (1994)

Farbig

Anmerkungen

The text is copied from the source, which is not given anywhere in the thesis. Some adaptations have taken place, which sometimes did not result in a coherent text (see first paragraph of this fragment).

[214.] Nm/Fragment 231 10

KomplettPlagiat

Untersuchte Arbeit: Seite: 231, Zeilen: 10-14	Quelle: Aviv et al 2003 Seite(n): 10, Zeilen: 5-8
The *cohesion index* is a measure of the degree to which there are strong links within the clique rather than outside of it (where the strength of a link reflects the number of responses exchanged along the link). If the cohesion index is greater than 1, then the links within the clique are stronger on average than the links with the [outside.]	The *Cohesion Index* is a measure of the degree to which there are strong links within the clique rather than outside of it (where the strength of a link reflects the number of responses exchanged along the link). If the cohesion is greater than 1, then the links within the clique are stronger on average than the links with the outside. A precise definition is given by Bock and Husain [40].

Farbig

Anmerkungen

As it is stated in the source: this is not a definition but an informal description. Nevertheless it appears word-for-word in Nm's thesis. No reference given.

[215.] Nm/Fragment 239 10

Verschleierung

Untersuchte Arbeit: Seite: 239, Zeilen: 10-20	Quelle: Hamill_2006 Seite(n): 278, Zeilen: 7-14
These measures could be useful for law enforcement and intelligence agencies to disrupt the effective operation and growth of these networks or destroy some terrorist cells entirely. Although these adversaries can be affected in a number of ways, this research focuses upon capturing / eradicating a terrorist organization's most influential persons or finding susceptible points of entry and conveying information or influence that contribute to winning the war against terrorism. This chapter provides a summary of methodological and practical contributions of this dissertation as well as recommendations for areas of future research.	Such opportunities lie within the ability to disrupt the effective operation and growth of these networks, or destroy them entirely. Although these adversaries can be affected in a number of ways, this research focuses upon either removing or mitigating an organization's most influential individuals, or finding susceptible points of entry and conveying information or influence that contributes to winning this war of ideas. This chapter provides a summary of the methodological and practical contributions of this dissertation, as well as recommendations for areas of future research.

Farbig

Anmerkungen

Even in the overview of the conclusions of the thesis there is copied text without referencing the original author.

[216.] Nm/Fragment 240 24

Verschleierung

Untersuchte Arbeit: Seite: 240, Zeilen: 24-26	Quelle: Hamill_2006 Seite(n): 278, Zeilen: 20-23
We assume that limited information that captured the dyadic interactions between terrorists was available. The models presented in this dissertation offer an [investigative data mining tool that lends itself to data-sparse environment initially confronted by law enforcement and intelligence agencies.]	The study begins with the assumption that limited information that captured the dyadic interactions between individuals was available. The methodology offers a screening tool that lends itself to the data-sparse environment initially confronted by analysts.

Farbig

Anmerkungen

The finding is quite short and has been adapted, but still, some text clearly has been copied without proper attribution.

[217.] Nm/Fragment 241 01

Verschleierung

Untersuchte Arbeit: Seite: 241, Zeilen: 1-3	Quelle: Hamill 2006 Seite(n): 278, Zeilen: 21-23	Farbig
[The models presented in this dissertation offer an] investigative data mining tool that lends itself to data-sparse environment initially confronted by law enforcement and intelligence agencies.	The methodology offers a screening tool that lends itself to the data-sparse environment initially confronted by analysts.	

Anmerkungen

this is the end of Nm/Fragment_240_24

[218.] Nm/Fragment 242 09

KomplettPlagiat

Untersuchte Arbeit: Seite: 242, Zeilen: 9-14	Quelle: Stephenson and Zelen 1989 Seite(n): 3, Zeilen: 28-33	Farbig
It is 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.	

Anmerkungen

Nearly identical, not marked as a citation, no reference given. See also Nm/Fragment_144_16.

[219.] Nm/Fragment 243 23

Verschleierung

Untersuchte Arbeit: Seite: 243, Zeilen: 23-26	Quelle: Saxena et al. 2004 Seite(n): 94, Zeilen: 11-15	Farbig
Further real-time or near real-time information from a multiplicity of databases could have the potential to generate early warning signals of utility in detecting and deterring terrorist attacks. It is necessary, of course, to have experts in the loop.	It has not escaped our notice that SNA, duly validated and used with real-time or near real-time information from a multiplicity of databases could have the potential to generate early warning signals of utility in detecting and deterring terrorist attacks. It is necessary, of course, to have ‘experts’ in the loop.	

Anmerkungen

Some conclusion is also taken from Saxena et al. 2004

[220.] Nm/Fragment 244 21

BauernOpfer

Untersuchte Arbeit: Seite: 244, Zeilen: 21-32	Quelle: Ressler 2006 Seite(n): 7, Zeilen: 25-34
Investigative data mining is just one tool that can be used to understand terrorism, and one piece of the puzzle. Domain experts are needed to provide a context for the research. Furthermore, the basic assumption of investigative data mining regarding terrorism may not be completely valid. Despite their non-hierarchical approach, terrorist organizations are not completely organized in a network structure (Ressler, S., 2006). There are still central headquarters and training camps for most terrorist organizations. Investigative data mining must attempt to address the underlying root cause of terrorism. It is helpful to understand how a network evolves and how to destabilize a network. It is more helpful, however, to understand how a network recruits human bombs and [why people wish to join terrorist networks.]	social network analysis is just one tool that can be used to understand terrorism, and is just one piece of the puzzle. Subject matter experts are needed to provide a context for the research. Furthermore, the basic assumption of network analysis regarding terrorism may not be completely valid. Despite their nonhierarchical approach, terrorist organizations are not completely organized in a network structure. There are still central headquarters and training facilities for most terrorist organizations. Also, social network analysis must attempt to address the underlying root cause of terrorism. It is helpful to understand how a network evolves and how to destabilize a network. It is more helpful, however, to understand how networks recruit participants and why people wish to join terrorist networks.

Farbig

Anmerkungen

Even at the end, when Nm tries to summarize his own results - we are talking about the section "9.2 DISSERTATION CONTRIBUTIONS" - there is a whole section from another work without it being marked as a citation. This paragraph originally belonged to the final - discussion - section of Ressler (2006).

The source Ressler (2006) is given, but no citation is marked (and the copied text continues after the reference to Ressler (2006)).

[221.] Nm/Fragment 245 01

Verschleierung

Untersuchte Arbeit: Seite: 245, Zeilen: 1-5	Quelle: Ressler 2006 Seite(n): 7, Zeilen: 32-37
[It is more helpful, however, to understand how a network recruits human bombs and] why people wish to join terrorist networks.	It is more helpful, however, to understand how networks recruit participants and why people wish to join terrorist networks.
It is believed to see an expansion of the research areas in which investigative data mining is being used with regard to terrorism. Only a limited amount of work has been completed and there is much room for this technology to yield insights into terrorism.	I would like to see an expansion of the research areas in which network analysis is being used with regard to terrorism. Only a limited amount of work has been completed, and there is much room for this tool to yield great insights into terrorism.

Farbig

Anmerkungen

Even final words are not Nm's own.

[222.] Nm/Fragment 246 08

Verschleierung

Untersuchte Arbeit: Seite: 246, Zeilen: 8-28	**Quelle: Lemieux_2003 Seite(n): 12-13, Zeilen: 12ff; 1ff**
[... the following roles in terrorist networks as proposed by Williams (2001):]	Williams (2001: 82-84) proposes the identification of a certain number of roles [...]
1) Organizers are the core ensuring a network's direction. They are the people who determine the scale and scope of activities, as well as the guidance and motivation necessary for performing those actions.	1) The organizers are the core ensuring the network's direction. It is they who determine the scale and scope of activities, as well as the guidance and impetus necessary for performing those activities.
2) Insulators are individuals or groups charged with insulating a core member from dangers posed by infiltration and cooperation situations to which it is exposed. These actors communicate commands or direction from a core member to a foot-soldier. They also ensure that the flow of communication from a foot soldier in no way compromises a core member.	2) Insulators are the individuals or groups charged with insulating the core from the danger posed by the infiltration and compromise to which it is exposed. These actors transmit directives or guidance from the core to the periphery. They also ensure that the flow of communication from the periphery in no way compromises the core.
3) Communicators are individuals who guarantee that message flows effectively from one actor to another throughout the network. Unlike insulators, communicators must collect response regarding directives that they transmit to other actors in a network. Williams claims that there can be conflicts between those who act as insulators and those who act as communicators, or that the same individuals may assume both roles simultaneously to avoid these conflicts.	3) Communicators are individuals who ensure that communication flows effectively [Page 13] from one actor to another throughout the network. Unlike the insulators, they must gather feedback regarding directives that they transmit to other actors in the network. Williams claims that there can be conflicts between those who act as insulators and those who act as communicators, or that the same individuals may assume both roles simultaneously to avoid these conflicts.
4) Guardians guarantee network security and take essential measures to diminish its vulnerability to infiltrations or external attack.	4) Guardians ensure network security and take necessary measures to minimize its vulnerability to infiltrations or external attack.

Anmerkungen

Williams (2001) is given as source, but this reference as well as many formulations are taken from Lemieux (2003) without reference.

In particular the sentence starting "Williams claims ..." is word by word taken from the source, which demonstrates that the text has been taken from Lemieux (2003) and not Williams (2001).

[223.] Nm/Fragment 247 01

Verschleierung

Untersuchte Arbeit: Seite: 247, Zeilen: 1-21	Quelle: Lemieux_2003 Seite(n): 13, Zeilen: 7ff	Farbig
[Their role also consists in watching over recruitment to a] network and ensuring the loyalty of recruits through a variety of procedural promises and hidden pressure directed against new members and their families. Guardians pursue to avoid defections from the network actors and to reduce losses when defections occur.	Their role also consists in watching over recruitment to the network and ensuring the loyalty of recruits through a variety of ritual oaths and latent coercion directed against new members and their families. Guardians seek to prevent defections from the network actors and to minimize damages when defections occur.	
5) Extenders extend the network by recruiting new members and also by negotiating association with other networks and encouraging association with the business sector, government and justice. Various strategies are used to this end. They range from unpaid recruitment through corruption and bribery to involuntary recruitment through pressure, infrequently supported by encouragements and prizes.	5) Extenders extend the network by recruiting new members and also by negotiating collaboration with other networks and encouraging collaboration with the business sector, government and justice. Various tactics are used to this end. They range from voluntary recruitment through bribery and corruption to involuntary recruitment through coercion, occasionally supported by incentives and rewards.	
6) Monitors are devoted to the network's usefulness their tasks consist in providing information to organizers regarding flaws and hitches within the network so that the organizers can decide them. Monitors guarantee that the network is able to correct to new situations and keep the high degree of elasticity that is essential to avoid law enforcement.	6) Monitors are dedicated to the network's effectiveness their responsibilities consist in providing information to organizers regarding weaknesses and problems within the network so that the organizers can resolve them. Monitors ensure that the network is able to adjust to new circumstances and maintain the high degree of flexibility that is necessary to circumvent law enforcement.	
7) Crossovers are part of a terrorist network, but continue to work in legal institutions, whether governmental, financial or commercial. As such, these individuals provide vital evidence and contribute to the guard of a network.	7) Crossovers are part of a criminal network, but continue to work in legal institutions, whether governmental, financial or commercial. As such, these individuals provide invaluable information and contribute to the protection of the network.	

Anmerkungen

Refer also to the previous page: Nm/Fragment_246_08. No source is given

[224.] Nm/Fragment 247 22

Verschleierung

Untersuchte Arbeit: Seite: 247, Zeilen: 22-29	Quelle: Ressler 2006 Seite(n): 7-8, Zeilen: p.7,45-46 - p.8,1-5	Farbig
Investigative data mining can also be used to understand the psychological effects of terrorism. One of the main effects of terrorism is fear, which is spread through network structures such as media, the Internet, and personal relationships. For example, the number of ties an individual has to victims of terrorism may impact the individual's perception of the risk of terrorism.	[p. 7] Network analysis can also be used to understand the psychological effect of terrorism. One of the main effects of terrorism is fear, which is spread through network	
It is believed to see further research on network structure evolution. It would be interesting to compare structures of multiple terrorist [networks to see how they evolve over time.]	[p.8] structures such as media, the Internet, and personal relationships. For example, the number of ties an individual has to victims of terrorism may impact the individual's perception of the risk of terrorism. Finally, I would like to see further research on network structure evolution. It would be interesting to compare the structure of multiple terrorist networks to see how they evolve over time.	

Anmerkungen

On the final stretch of Nm's thesis one can find a large portion of somebody else's final thoughts on the subject.

[225.] Nm/Fragment 248 01

Verschleierung

Untersuchte Arbeit: Seite: 248, Zeilen: 1-9	Quelle: Ressler 2006 Seite(n): 8, Zeilen: 5-11
The network structure may impact the ability of an organization to endure over the years and to complete attacks. It is important for intelligence agencies to understand how to fragment a network; they could potentially exploit the destabilizing techniques discussed in this research work including small world topology by eliminating weak ties in order to isolate the network and diminish its reach and power. The removal of individuals in key network regions may be even more important than attacking the traditional leaders of a group.	The network structure may impact the ability of an organization to endure over the years and complete attacks. It is important for intelligence analysts to understand how to break up a network; they could potentially exploit the small world topology by eliminating weak ties in order to isolate the network and diminish its reach and power. The removal of individuals in key network locations may be even more important than attacking the traditional leaders of a group.

Farbig

Anmerkungen

continued from previous page

[226.] Nm/Fragment 248 24

Verschleierung

Untersuchte Arbeit: Seite: 248, Zeilen: 24-28	Quelle: Hamill_2006 Seite(n): 285, Zeilen: 10-14
Considering the nature of this war, understanding the structure of these networks is paramount. No longer fitting the traditional paradigm of combat between great armies, this war involves not only defeating the individuals actively threatening National Security, but also alleviating the environments that nurture the [development and continuity of such groups.]	Considering the nature of this war, understanding the enemy is paramount. No longer fitting the traditional paradigm of combat between great armies, this war involves not only defeating the individuals actively threatening our National Security, but also mitigating the environments that nurture the development and continuity of such groups.

Farbig

Anmerkungen

Even the final summary is copied from somewhere else.

[227.] Nm/Fragment 249 01

Verschleierung

Untersuchte Arbeit: Seite: 249, Zeilen: 1-8	Quelle: Hamill_2006 Seite(n): 285, Zeilen: 14-19
In order to accomplish this, analysts must at minimum (1) improve the understanding why people would undertake such activities and mentally prepare to be used as human bombs; (2) identify vulnerabilities existing within these networks and how to exploit them; and, (3) determine what consequences may follow an operation to minimize the likelihood that actions executed unintentionally contribute to the environments that promote extremism.	In order to accomplish this, the appropriate communities must at a minimum (1) improve the understanding of why people would undertake such activities; (2) identify limitations or vulnerabilities existing within non-cooperative networks and how to exploit them; and, (3) determine what repercussions may follow an operation to minimize the likelihood that actions executed inadvertently contribute to the environments that promote extremism.

Farbig

Anmerkungen

Not even the last words of the thesis are from the author

Sources (Quellen)

[1.] Quelle:Nm/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:Nm/Aviv et al 2003

Autor	Aviv, Reuven; Erlich, Zippy; Ravid, Gilad; Geva, Aviva
Titel	Network Analysis of Knowledge Construction in Asynchronous Learning Networks
Zeitschrift	Journal of Asynchronous Learning Networks
Verlag	The Sloan Consortium
Jahr	2003
Nummer	7 (3)
URL	http://sloanconsortium.org/sites/default/files/v7n3_aviv_1.pdf
Literaturverz.	no
Fußnoten	no

[3.] Quelle:Nm/Balasundaram et al 2006

Autor	B. Balasundaram, S. Butenko, I. V. Hicks, S. Sachdeva
Titel	Clique Relaxations in Social Network Analysis: The Maximum k-plex Problem
Datum	27. January 2006
Anmerkung	Date according to PDF file properties
URL	http://www.caam.rice.edu/~ivhicks/kplex.general.pdf
Webcite	http://www.webcitation.org/6MzMGGm2A
Literaturverz.	no
Fußnoten	no

[4.] Quelle:Nm/Bedi 2005

Autor	Rohan Bedi
Titel	Telecom - The Terrorism Risk
Herausgeber	International Centre for Political Violence and Terrorism Research - IDSS Singapore
Ort	Singapore
Datum	26. September 2005
URL	http://www.pvtr.org/pdf/Financial%20Response/Telecom%20-%20The%20Terrorism%20Risk.pdf
Literaturverz.	yes
Fußnoten	yes

[5.] Quelle:Nm/Berry etal 2004

Autor	Nina Berry, Teresa Ko, Tim Moy, Julienne Smrcka, Jessica Turnley, Ben Wu
Titel	Emergent Clique Formation in Terrorist Recruitment
Sammlung	The AAAI-04 Workshop on Agent Organizations: Theory and Practice
Datum	July. 25 2004
URL	http://www.aaai.org/Papers/Workshops/2004/WS-04-02/WS04-02-005.pdf
Literaturverz.	yes
Fußnoten	yes (in text)

[6.] Quelle:Nm/Borgatti 2002

Autor	Stephen P. Borgatti
Titel	Graph Theory
Jahr	2002
Anmerkung	Notes from the CASOS Institute 2002 - Reading List; NM hat den identischen Text auch 2008 publiziert: http://nguyendangbinh.org/Proceedings/IPCV08/Papers/ICA4831.pdf
URL	http://www.casos.cs.cmu.edu/events/summer_institute/2002/reading_list/borgatti/graphtheory.pdf
Literaturverz.	no
Fußnoten	no

[7.] Quelle:Nm/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

[8.] Quelle:Nm/CNS 2002

Titel	LITERATURE REVIEW OF EXISTING TERRORIST BEHAVIOR MODELING Final Report to the Defense Threat Reduction Agency
Herausgeber	Center for Nonproliferation Studies
Beteiligte	Amy Sands, Jason Pate, Gary Ackerman, Anjali Bhattacharjee, Matthew Klag, Jennifer Mitchell
Datum	14. August 2002
URL	http://cns.miis.edu/reports/pdfs/terror_lit.pdf
Literaturverz.	no
Fußnoten	no

[9.] Quelle:Nm/Carley 2006

Autor	Kathleen M. Carley
Titel	Destabilization of covert networks
Zeitschrift	Comput Math Organiz Theor
Jahr	2006
Nummer	12
Seiten	51-66
DOI	DOI 10.1007/s10588-006-7083-y
URL	http://www.springerlink.com/content/p17u819571885670/
Literaturverz.	no
Fußnoten	no

[10.] Quelle:Nm/Chen 2006

Autor	Hsinchun Chen
Titel	Intelligence and Security Informatics for International Security: Information Sharing and Data Mining
Verlag	Springer-Verlag
Jahr	2006
URL	http://ai.arizona.edu/mis596a/
Literaturverz.	yes
Fußnoten	yes

[11.] Quelle:Nm/Clark etal 2005

Autor	Clinton R. Clark, Richard F. Deckro, Jeffrey D. Weir, Marcus B. Perry
Titel	Modeling and Analysis of Clandestine Networks
Datum	15. December 2005
Anmerkung	Barchi Prize Submission
URL	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA444968
Literaturverz.	no
Fußnoten	no

[12.] Quelle:Nm/Clauset Young 2005

Autor	Aaron Clauset, Maxwell Young
Titel	Scale Invariance in Global Terrorism
Datum	30. April 2005
Anmerkung	see also: arxiv (http://arxiv.org/abs/physics/0502014)
URL	http://www.cs.unm.edu/~moore/tr/05-05/terrorism.pdf
Literaturverz.	nein
Fußnoten	ja

[13.] Quelle:Nm/Combating Terrorism Center 2006

Titel	Harmony and Disharmony - Exploiting al-Qa'ida's Organizational Vulnerabilities
Herausgeber	Combating Terrorism Center, Department of Social Sciences, United States Military Academy
Ort	West Point, NY, USA
Datum	14. February 2006
Seiten	116
Anmerkung	An alternative source is the publication: "The Terrorist's Challenge: Security, Efficiency, Control" by Jacob N. Shapiro (2007) [9] (http://igcc3.ucsd.edu/pdf/Shapiro.pdf)
URL	http://iis-db.stanford.edu/pubs/21057/Harmony_and_Disharmony-CTC.pdf
Literaturverz.	no
Fußnoten	no

[14.] Quelle:Nm/DCSINT 2005

Titel	TRADOC DCSINT Handbook No. 1. A Military Guide to Terrorism in the Twenty-First Century
Herausgeber	US Army Training and Doctrine Command
Ort	Fort Leavenworth, Kansas
Ausgabe	Version 3.0
Datum	15. August 2005
URL	http://web.archive.org/web/20060110065831/http://www.fas.org/irp/threat/terrorism/index.html
Literaturverz.	no
Fußnoten	yes

[15.] Quelle:Nm/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

[16.] Quelle:Nm/Dombroski Carley 2002

Autor	Matthew J. Dombroski, Kathleen M. Carley
Titel	NETEST: Estimating a Terrorist Network's Structure
Sammlung	CASOS conference proceedings
Ort	Pittsburgh, PA.
Jahr	2002
URL	http://www.casos.cs.cmu.edu/publications/working_papers/Dombroski-CASOS-02.pdf
Literaturverz.	yes
Fußnoten	no

[17.] Quelle:Nm/Dugan etal 2006

Autor	Laura Dugan, Gary LaFree, Heather Fogg
Titel	A First Look at Domestic and International Global Terrorism Events, 1970–1997
Sammlung	Intelligence and Security Informatics: IEEE International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006 : Proceedings
Herausgeber	Sharad Mehrotra, Daniel D. Zeng, Hsinchun Chen, Bhavani Thuraisingham, Fei-Yue Wang
Ort	Berlin Heidelberg
Verlag	Springer-Verlag
Jahr	2006
Seiten	407-419
ISBN	3-540-34478-0
ISSN	0302-9743
URL	[10] (http://www.springerlink.com/content/g26p24152m696wx9/) and Google books (http://books.google.de /books?id=kF1jS9Nn8HUC)
Literaturverz.	no
Fußnoten	no

[18.] Quelle:Nm/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

[19.] Quelle:Nm/Frost 1982

Autor	R.A. Frost
Titel	Binary-Relational Storage Structures
Zeitschrift	The Computer Journal
Verlag	Heyden & Son Ltd
Jahr	1982
Nummer	25 (3)
Seiten	358-367
DOI	10.1093/comjnl/25.3.358
URL	comjnl.oxfordjournals.org/content/25/3/358.full.pdf
Literaturverz.	yes
Fußnoten	yes

[20.] Quelle:Nm/Hamill 2006

Autor	Jonathan T. Hamill
Titel	Analysis of layered social networks
Datum	September 2006
Anmerkung	Dissertation at AIR FORCE INSTITUTE OF TECHNOLOGY
URL	http://www.au.af.mil/au/awc/awcgate/afit/hamill_layered_social_networks.pdf
Literaturverz.	no
Fußnoten	no

[21.] Quelle:Nm/Han Kamber 2006

Autor	Jiawei Han, Micheline Kamber
Titel	Data Mining: Concepts and Techniques (second edition)
Ort	San Francisco
Verlag	Morgan Kaufmann, Elsevier
Jahr	2006
ISBN	1-55860-901-6
URL	http://books.google.es/books?id=AfL0t-YzOrEC
Literaturverz.	no
Fußnoten	no

[22.] Quelle:Nm/Heer et al 2005

Autor	Jeffrey Heer, Stuart K. Card, James A. Landay
Titel	**prefuse**: a toolkit for interactive information visualization
Sammlung	CHI '05: Proceedings of the SIGCHI conference on Human factors in computing systems - Portland, OR, USA — April 02 - 07, 2005
Herausgeber	ACM
Ort	New York
Jahr	2005
Seiten	421-430
DOI	10.1145/1054972.1055031
URL	http://web.cs.dal.ca/~sbrooks/csci4166-6406/seminars/readings/Heer_Prefuse_CHI05.pdf
Literaturverz.	no
Fußnoten	yes

[23.] Quelle:Nm/Holmgren 2006

Autor	Åke J. Holmgren
Titel	Using Graph Models to Analyze the Vulnerability of Electric Power Networks
Zeitschrift	Risk Analysis
Verlag	Wiley
Jahr	2006
Nummer	26 (4)
Seiten	955-969
DOI	10.1111/j.1539-6924.2006.00791.x
URL	http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2006.00791.x/abstract?
Literaturverz.	no
Fußnoten	no

[24.] Quelle:Nm/Jensen et al 2003

Autor	David Jensen, Matthew Rattigan, Hannah Blau
Titel	Information Awareness: A Prospective Technical Assessment
Sammlung	Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; SIGKDD '03, August 24-27, 2003, Washington, DC, USA
Jahr	2003
Seiten	378-387
DOI	10.1.1.75.9486
URL	citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.9486&rep=rep1&type=pdf
Literaturverz.	no
Fußnoten	no

[25.] Quelle:Nm/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	[11] (http://sgr.sagepub.com/content/35/3/307) , [12] (http://www.hks.harvard.edu/davidlazer/files/papers /Lazer_Katz_Small_Group.pdf)
Literaturverz.	yes
Fußnoten	yes

[26.] Quelle:Nm/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

[27.] Quelle:Nm/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

[28.] Quelle:Nm/Koschuetzki etal 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

[29.] Quelle:Nm/Krebs 2002

Autor Krebs, Valdis E.
Titel Mapping Networks of Terrorist Cells
Zeitschrift Connections
Jahr 2002
Nummer 24 (3)
Seiten 43-52
URL http://vlado.fmf.uni-lj.si/pub/networks/doc/Seminar/Krebs.pdf

Literaturverz. yes
Fußnoten no

[30.] Quelle:Nm/Krebs 2004

Autor Valdis Krebs
Titel Organizational Hierarchy - Adapting Old Structures to New Challenges
Jahr 2004
URL http://web.archive.org/web/20040818093318/http://www.orgnet.com/orgchart.html

Literaturverz. yes
Fußnoten yes

[31.] Quelle:Nm/Latora and Marchiori 2004

Autor Vito Latora, Massimo Marchiori
Titel How the science of complex networks can help developing strategies against terrorism
Zeitschrift Chaos, Solitons and Fractals
Verlag Elsevier
Jahr 2004
Nummer 20
Seiten 69-75
DOI 10.1016/S0960-0779(03)00429-6
URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.3998&rep=rep1&type=pdf

Literaturverz. yes
Fußnoten yes

[32.] Quelle:Nm/Lemieux 2003

Autor Vincent Lemieux
Titel Criminal Networks
Ort Ottawa
Jahr 2003
ISBN 0-662-67645-9
URL http://cpc.phippsinc.com/cpclib/pdf/56312e.pdf

Literaturverz. no
Fußnoten no

[33.] Quelle:Nm/Malin etal 2005

Autor Bradley Malin, Edoardo Airoldi, Kathleen M. Carley
Titel A Network Analysis Model for Disambiguation of Names in Lists
Zeitschrift COMPUTATIONAL & MATHEMATICAL ORGANIZATION THEORY
Verlag Springer
Ausgabe 11
Datum July 2005
Nummer 2
Seiten 119-139
URL http://www.casos.cs.cmu.edu/publications/papers/networkanalysismodel.pdf

Literaturverz. no
Fußnoten no

[34.] Quelle:Nm/Padhy 2006

Autor Prafullah Padhy
Titel Organised Crime
Ort Delhi (India)
Verlag Isha Books
Jahr 2006
Anmerkung Chapter 7 "Organised Crime and Terrorism" is nothing else but an americanized copy of Shelley (2002).
ISBN 81-8205-348-X
URL http://books.google.de/books?id=mgIqP8dEwCMC&printsec=frontcover&hl=de#v=onepage&q&f=false

[35.] Quelle:Nm/Penzar etal 2005

Autor Dražen Penzar, Armano Srbljinović
Titel About Modelling of complex networks with applications to terrorist group modelling
Zeitschrift Interdisciplinary Description of Complex Systems
Jahr 2005
Jahrgang 3
Nummer 1
Seiten 27-43
ISSN 1334-4676
URL http://www.indecs.eu/2005/indecs2005-pp27-43.pdf

Literaturverz. no
Fußnoten no

[36.] Quelle:Nm/Perer Shneiderman 2006

Autor	Adam Perer, Ben Shneiderman
Titel	Balancing Systematic and FlexibleExploration of Social Networks
Zeitschrift	IEEE Transactions on visualization and computer graphics
Verlag	IEEE Computer Society
Datum	September/October 2006
Jahrgang	12
Nummer	5
Seiten	693-700
Anmerkung	The freely downloadable version of the paper contains no page numbers. Those can be inferred easily, however, as paper contains 8 pages.
ISSN	1077-2626
URL	http://hcil.cs.umd.edu/trs/2006-25/2006-25.pdf
Literaturverz.	no
Fußnoten	no

[37.] Quelle:Nm/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.	ja
Fußnoten	nein

[38.] Quelle:Nm/Qin et al 2005

Autor	Jialun Qin, Jennifer J. Xu, Daning Hu, Marc Sageman, Hsinchun Chen
Titel	Analyzing Terrorist Networks: A Case Study of the Global Salafi Jihad Network
Sammlung	Intelligence and Security Informatics 2005
Herausgeber	Kantor, P et al.
Ort	Berlin, Heidelberg
Verlag	Springer-Verlag
Jahr	2005
Nummer	3495
Seiten	287-304
Reihe	Lecture Notes in Computer Science
DOI	10.1007/11427995_24
URL	http://www.springerlink.com/content/vca9dpldq8ue8dfu/
Literaturverz.	yes
Fußnoten	yes

[39.] Quelle:Nm/Ressler 2006

Autor	Steve Ressler
Titel	Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research
Zeitschrift	Homeland Security Affairs
Herausgeber	Naval Postgraduate School Center for Homeland Defense and Security
Datum	July 2006
Nummer	2 (2)
URL	http://www.hsaj.org/?fullarticle=2.2.8
Literaturverz.	yes
Fußnoten	yes

[40.] Quelle:Nm/Saxena et al. 2004

Autor	Sudhir Saxena, K. Santhanam, Aparna Basu
Titel	Application of Social Network Analysis (SNA) to Terrorist Networks in Jammu & Kashmir
Zeitschrift	Strategic Analysis
Herausgeber	Institute for Defence Studies and Analyses
Ausgabe	28
Datum	Jan-Mar 2004
Nummer	1
Seiten	84-101
URL	http://www.idsa.in/system/files/strategicanalysis_ksanthanam_0304.pdf
Literaturverz.	no
Fußnoten	no

[41.] Quelle:Nm/Scott 1987

Autor	John Scott
Titel	Social network analysis, a Handbook
Ort	London
Verlag	Sage Publications
Jahr	1987
Anmerkung	Nm gives the second edition in the bibliography. Used here is the first edition (available via weblink)
URL	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CFUQFjAG&url=http%3A%2F%2Fsocio.ens-lyon.fr%2Fagregation%2Freseaux%2Freseaux_fiches_scott_1987_extraits.doc&ei=eHGWT6WCN4S2hAfm1tHZDQ&usg=AFQjCNG5Z424hgZUqByhrAV7CfIsonfj9g
Literaturverz.	yes
Fußnoten	yes

[42.] Quelle:Nm/Shelley 2002

Autor	Louise I. Shelley
Titel	The Nexus of Organized International Criminals and Terrorism
Zeitschrift	International Annals of Criminology
Herausgeber	International Society for Criminology (ISC)
Jahr	2002
Seiten	85-92
Anmerkung	The www-version differs in the numbering of pages.
URL	http://beepdf.com/doc/39511/the_nexus_of_organized_international_criminals_and_terrorism.html
Literaturverz.	no
Fußnoten	yes

[43.] Quelle:Nm/Shelley Picarelli 2002

Autor	Shelley, Louise I. and Picarelli, John T.
Titel	Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism
Zeitschrift	Police Practice and Research:An International Journal
Jahr	2002
Nummer	3
Seiten	305-318
DOI	10.1080/1561426022000032079
URL	http://www.law.syr.edu/Pdfs/0methods_motives.pdf
Literaturverz.	no
Fußnoten	yes

[44.] Quelle:Nm/Smith and King 2002

Autor	M.N. Smith, P.J.H. King
Titel	The Exploratory Construction of Database Views
Herausgeber	School of Computer Science and Information Systems, Birbeck College, University of London
Ort	London
Jahr	2002
Nummer	02-02
Umfang	11 Seiten
Reihe	Research Report BBKCS
Anmerkung	It has already been officially noted in 2009 (see [13] (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5066528)) that Nm has taken parts of this source for yet another of his papers with "insufficient attribution (including appropriate references to the original author(s) and/or paper titles) and without permission".
URL	http://www.dcs.bbk.ac.uk/TriStarp/pubs/ECoDV2002.pdf
Literaturverz.	no
Fußnoten	no

[45.] Quelle:Nm/Stephenson and Zelen 1989

Autor	Stephenson, Karen and Zelen, Marvin
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.	ja
Fußnoten	nein

[46.] Quelle:Nm/Stokman 2004

Autor	Frans N. Stokman
Titel	What Binds Us When With Whom? Content and Structure in Social Network Analysis
Datum	December 2004
Anmerkung	Extended version of keynote at the SUNBELT XXIV May 13, 2004
URL	http://www.stokman.org/artikel/04Stok.WhatBinds.ISNC.pdf
Literaturverz.	no
Fußnoten	no

[47.] Quelle:Nm/The Dark Web Project 2010

Autor	University of Arizona
Titel	Dark Web Terrorism Research
Herausgeber	University of Arizona
Ort	Arizona
Verlag	University of Arizona
Jahr	2010
Seiten	1 (internetquelle)
Anmerkung	Quelle kann nicht datiert werden. web.archive.org zeigt 2010 an.
URL	http://ai.eller.arizona.edu/research/terror/
Literaturverz.	nein
Fußnoten	nein

[48.] Quelle:Nm/TrackingTheThreat.com 2006

Titel	About this site
Datum	6. May 2006
URL	http://web.archive.org/web/20060506170745/http://www.trackingthethreat.com/about/
Literaturverz.	no
Fußnoten	yes

[49.] Quelle:Nm/TrackingTheThreat.com 2006a

Titel	About TrackingTheThreat.com
Datum	6. May 2006
URL	http://web.archive.org/web/20060506170452/http://www.trackingthethreat.com/index.jsp
Literaturverz.	no
Fußnoten	yes

[50.] Quelle:Nm/Tsvetovat et al. 2005

Autor	Maksim Tsvetovat, Jana Diesner, Kathleen M. Carley
Titel	NetIntel: A Database for Manipulation of Rich Social Network Data
Datum	3. March 2005
Anmerkung	Carnegie Mellon University School of Computer Science ISRI - Institute for Software Research International CASOS - Center for Computational Analysis of Social and Organizational Systems: CMU-ISRI-04-135
URL	http://www.docstoc.com/docs/4199494/NetIntel-A-Database-for-Manipulation-of-Rich-Social-Network
Literaturverz.	no
Fußnoten	no

[51.] Quelle:Nm/Visualcomplexity 2006

Titel	TrackingTheThreat.com
Herausgeber	www.visualcomplexity.com
Jahr	2006
URL	http://web.archive.org/web/20060629224345/http://www.visualcomplexity.com/vc/project.cfm?id=317
Literaturverz.	no
Fußnoten	no

[52.] Quelle:Nm/Westphal and Blaxton 1998

Autor	Christopher Westphal, Teresa Blaxton
Titel	Data Mining Solutions: Methods and Tools for Solving Real-World Problems
Ort	New York
Verlag	John Wiley & Sons, Inc
Jahr	1998
ISBN	0-471-25384-7
URL	http://www.amazon.com/Data-Mining-Tools-Action-Toolkits/dp/0471253847/ref=sr_1_1?ie=UTF8&qid=1338577210&sr=8-1
Literaturverz.	no
Fußnoten	no

[53.] Quelle:Nm/Wikipedia-Bojinka-plot 2006

Titel	Bojinka plot
Sammlung	Wikipedia
Datum	10. July 2006
URL	http://en.wikipedia.org/w/index.php?title=Bojinka_plot&oldid=62959798
Literaturverz.	no
Fußnoten	no

[54.] Quelle:Nm/Wikipedia - Adnan Gulshair el Shukrijumah - 2006

Titel	Adnan Gulshair el Shukrijumah
Sammlung	Wikipedia
Datum	June 2006
URL	http://en.wikipedia.org/w/index.php?title=Adnan_Gulshair_el_Shukrijumah&oldid=56448809
Literaturverz.	no
Fußnoten	yes

[55.] Quelle:Nm/Wikipedia - World Trade Center bombing (1993) - 2006

Titel	World Trade Center bombing (1993)
Sammlung	Wikipedia
Datum	September 2006
URL	http://en.wikipedia.org/w/index.php?title=World_Trade_Center_bombing_%281993%29&oldid=75731079
Literaturverz.	no
Fußnoten	yes

[56.] Quelle:Nm/Wikipedia Riyadh compound bombings 2007

Titel	Riyadh compound bombings
Datum	11. February 2007
URL	http://en.wikipedia.org/w/index.php?title=Riyadh_compound_bombings&oldid=107404494
Literaturverz.	no
Fußnoten	yes

[57.] Quelle:Nm/WorldNetDaily - Wheeler 2003

Autor	Scott L. Wheeler
Titel	'Dirty-bomb' plot under way in U.S.? - Fears over elusive al-Qaida suspect, missing reactor materials
Zeitschrift	WorldNetDaily
Datum	30. October 2003
URL	http://www.wnd.com/2003/10/21524/
Literaturverz.	nein
Fußnoten	nein

[58.] Quelle:Nm/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-Verlag
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.	yes
Fußnoten	yes

[59.] Quelle:Nm/Xu and Chen 2005a

Autor	Jennifer Xu, Hsinchun Chen
Titel	Criminal Network Analysis and Visualization: A Data Mining Perspective
Zeitschrift	Communications of the ACM (CACM)
Datum	June 2005
Nummer	48 (6)
Seiten	101-107
DOI	10.1145/1064830.1064834
URL	http://dl.acm.org/citation.cfm?id=1064830.1064834&coll=portal&dl=ACM; http://ai.bpa.arizona.edu/coplink/publications/crimenet/Xu_CACM.doc
Literaturverz.	no
Fußnoten	no

[60.] Quelle:Nm/Xu and Chen 2005b

Autor	Jennifer J. Xu, Hsinchun Chen
Titel	CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery
Zeitschrift	ACM Transactions on Information Systems
Datum	April 2005
Nummer	23 (2)
Seiten	201–226
Anmerkung	to be found as a reference in Nm, but with a wrong year
DOI	10.1145/1059981.1059984
URL	http://dl.acm.org/citation.cfm?id=1059984; http://comminfo.rutgers.edu/~muresan/IR/Docs/Articles/toisXu2005.pdf
Literaturverz.	yes
Fußnoten	yes

[61.] Quelle:Nm/Xu etal 2004

Autor	Jennifer Xu, Byron Marshall, Siddharth Kaza, Hsinchun Chen
Titel	Analyzing and Visualizing Criminal Network Dynamics: A Case Study
Jahr	2004
Anmerkung	The article has been published also in: Intelligence and Security Informatics: Second Symposium on Intelligence and Security Informatics, ISI 2004, Tucson, AZ, USA, June 10-11, 2004 ; Proceedings, Band 2, Editor: Hsinchun Chen, ISBN 3-540-22125-5, Springer-Verlag Berlin, Pages 359-377 Google Books (http://books.google.de /books?id=zfvf37_YS8cC&pg=PA360&lpg=PA360& dq=A+terrorist+network+is+primarily+a+social+network+in+which+individuals+connect+with+one+another+through& source=bl&ots=L9QluRgzaD&sig=eFOSN9HkfwI6CmrAcxT-Iqve_6w&hl=de&sa=X&ei=QC-GT4HwGYeR0AWPqbXMBw&ved=0CCgQ6AEwAA#v=onepage& q=Dynamic%20criminal%20network%20analysis%20is%20important%20for%20national%20security&f=false) , the page numbers given here refer to the version that is available online.
URL	http://ai.arizona.edu/intranet/papers/isi2004networkdynamics.pdf
Literaturverz.	no
Fußnoten	no

[62.] Quelle:Nm/Yang etal 2005

Autor	Huijie Yang, Wenxu Wang, Tao Zhou, Binghong Wang, Fangcui Zhao
Titel	Reconstruct the Hierarchical Structure in a Complex Network
Zeitschrift	arxiv.org
Datum	3. August 2005
URL	http://arxiv.org/abs/physics/0508026v1

[63.] Quelle:Nm/Zhao et al 2006

Autor	Bin Zhao, Prithviraj Sen, Lise Getoor
Titel	Entity and Relationship Labeling in Affiliation Networks
Sammlung	Proceedings of the 23 rd International Conference on Machine Learning, Pittsburgh, PA, 2006
Ort	Pittsburgh
Jahr	2006
URL	http://www.mindswap.org/papers/2006/RelClzPIT.pdf
Literaturverz.	no
Fußnoten	no

[64.] Quelle:Nm/terrorism research 2005

Titel	terrorism research
Jahr	2005
Anmerkung	On the website it says: [The information found on this web site] is derived from various US Government documents and open source/public domain material
URL	http://web.archive.org/web/20050125174021/http://www.terrorism-research.com/groups/
Literaturverz.	no
Fußnoten	no