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


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

**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:
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://nyhederen.tv2.dk/article.php?id=50105993;forsker-mist%C3%A6nk-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 in the VroniPlag Wiki was not the same 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:
  - 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.
  - 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_249_01. The first sentences of the thesis are also copied (but from another source): Nm/Fragment_019_01
- Others (co-authored by Chen) are also among the not sufficiently referenced sources: Xu & Chen (2003), Chen (2006), Xu & Chen (2005a), Xu & Chen (2005b)
- In many instances the copied text is adapted to make it more suitable for the terrorist theme of the thesis, often substituting the word "terrorists" for "criminals". Some examples are given here:
  - Nm/Fragment_194_01
  - Nm/Fragment_019_01

**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 titles?

- **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/*
- **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&dq=%22variation+seen+in+the+participation+index+we+conclude+that%22&source=bl&ots=X2YiaZEqG6&sig=1V9jBPGcCnSHtTvM6tR8xEPpE&hl=en&sa=X&ved=1kycT8ytMoOtOQQ9eX2Dg&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 „Komplettplagiat“). 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:

<table>
<thead>
<tr>
<th>Percentage plagiarism</th>
<th>Number of pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>No plagiarism documented</td>
<td>81</td>
</tr>
<tr>
<td>0%-50% Plagiarism</td>
<td>43</td>
</tr>
<tr>
<td>50%-75% Plagiarism</td>
<td>19</td>
</tr>
<tr>
<td>75%-100% Plagiarism</td>
<td>88</td>
</tr>
</tbody>
</table>

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).

- UP = Translation plagiarism,
- KP = Copy and paste,
- VS = Disguised plagiarism,
- BO = Pawn sacrifice,
- KW = No opinion,
- KeinP = Not plagiarism.
<table>
<thead>
<tr>
<th>Source</th>
<th>Year</th>
<th>ÜP</th>
<th>KP</th>
<th>VS</th>
<th>BO</th>
<th>KW</th>
<th>KeinP</th>
<th>Σ</th>
<th>To be reviewed</th>
<th>In progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arquilla Ronfeldt</td>
<td>2001</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Aviv et al</td>
<td>2003</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Balasundaram et al</td>
<td>2006</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bedi</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Berry et al</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Borgatti</td>
<td>2002</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Brandes Erlebach</td>
<td>2005</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CNS</td>
<td>2002</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Carley</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Chen</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Clark et al</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Clauset Young</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Combating Terrorism Center</td>
<td>2006</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DCSINT</td>
<td>2005</td>
<td>0</td>
<td>1</td>
<td>18</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DeRosa</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dombroski Carley</td>
<td>2002</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dugan et al</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Freeman</td>
<td>1980</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Frost</td>
<td>1982</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hamill</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Han Kamber</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Heer et al</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Holmgren</td>
<td>2006</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jensen et al</td>
<td>2003</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Katz et al</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Koelle et al</td>
<td>2006</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Koschade</td>
<td>2005</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Koschuetzki et al</td>
<td>2005</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Krebs</td>
<td>2002</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Krebs</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Latora and Marchiori</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Lemieux</td>
<td>2003</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Malin et al</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Padhy</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Penzar et al</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Perer Shneiderman</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Popp and Poindeexter</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Qin et al</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ressler</td>
<td>2006</td>
<td>0</td>
<td>2</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Saxena et al</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scott</td>
<td>1987</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Shelley</td>
<td>2002</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Shelley Picarelli</td>
<td>2002</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Smith and King</td>
<td>2002</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Stephenson and Zelen</td>
<td>1989</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Stokman</td>
<td>2004</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>The Dark Web Project</td>
<td>2010</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>TrackingTheThreat.com</td>
<td>2006</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TrackingTheThreat.com</td>
<td>2006a</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Source</td>
<td>Year</td>
<td>ÜP</td>
<td>KP</td>
<td>VS</td>
<td>BO</td>
<td>KW</td>
<td>KeinP</td>
<td>Σ</td>
<td>To be reviewed</td>
<td>In progress</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>-------</td>
<td>---</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Tsvetovat et al.</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Visualcomplexity</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Westphal and Blaxton</td>
<td>1998</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wikipedia - Adnan Gulshair el Shukrijumah -</td>
<td>2006</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wikipedia - World Trade Center bombing (1993) -</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wikipedia Riyadh compound bombings</td>
<td>2007</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wikipedia-Bojinka-plot</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WorldNetDaily - Wheeler</td>
<td>2003</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Xu and Chen</td>
<td>2003</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Xu and Chen</td>
<td>2005a</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Xu and Chen</td>
<td>2005b</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Xu etal</td>
<td>2004</td>
<td>0</td>
<td>1</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yang etal</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zhao et al</td>
<td>2006</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>terrorism research</td>
<td>2005</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Σ</td>
<td>-</td>
<td>0</td>
<td>30</td>
<td>171</td>
<td>26</td>
<td>6</td>
<td>0</td>
<td>233</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

**Fragments**

227 reviewed fragments
<table>
<thead>
<tr>
<th>Fragment</th>
<th>SeiteArbeit</th>
<th>ZeileArbeit</th>
<th>Quelle</th>
<th>SeiteQuelle</th>
<th>Typus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nm/Fragment</td>
<td>019 01</td>
<td>19</td>
<td>1, 3-15</td>
<td>Xu and Chen 2003</td>
<td>232 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>019 16</td>
<td>19</td>
<td>16-25</td>
<td>Katz et al 2004</td>
<td>308-309 BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>020 01</td>
<td>20</td>
<td>1-23</td>
<td>Katz et al 2004</td>
<td>308-309 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>021 01</td>
<td>21</td>
<td>1-5</td>
<td>Xu and Chen 2003</td>
<td>233 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>023 27</td>
<td>23</td>
<td>27-30</td>
<td>DeRosa 2004</td>
<td>v BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>024 01</td>
<td>24</td>
<td>4-20</td>
<td>DeRosa 2004</td>
<td>v BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>025 22</td>
<td>25</td>
<td>22-29</td>
<td>Koschade_2005</td>
<td>2, 3 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>025 30</td>
<td>25</td>
<td>30-32</td>
<td>DeRosa 2004</td>
<td>6 BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>026 01</td>
<td>26</td>
<td>1-3</td>
<td>DeRosa 2004</td>
<td>6 BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>026 04</td>
<td>26</td>
<td>4-13</td>
<td>Koschade_2005</td>
<td>2, 3 KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td>026 14</td>
<td>26</td>
<td>14-23</td>
<td>Popp and Poindexter 2006</td>
<td>23 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>028 05</td>
<td>28</td>
<td>5-8</td>
<td>Xu and Chen 2005a</td>
<td>102 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>028 08</td>
<td>28</td>
<td>8-27</td>
<td>Koelle et al 2006</td>
<td>1 (internet version) KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td>029 03</td>
<td>29</td>
<td>3-8</td>
<td>Tsvetovat et al. 2005</td>
<td>cover Verschleierung</td>
</tr>
<tr>
<td></td>
<td>029 24</td>
<td>29</td>
<td>24-27</td>
<td>DeRosa 2004</td>
<td>6 BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>030 01</td>
<td>30</td>
<td>1-26</td>
<td>DeRosa 2004</td>
<td>6-7 BauernOpfer</td>
</tr>
<tr>
<td></td>
<td>031 15</td>
<td>31</td>
<td>15-27</td>
<td>Han_Kamber_2006</td>
<td>560, 561, 562 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>032 02</td>
<td>32</td>
<td>2-10</td>
<td>Han_Kamber_2006</td>
<td>561, 562 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>033 01</td>
<td>33</td>
<td>1-15</td>
<td>Koelle et al 2006</td>
<td>1 (internet version) KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td>033 15</td>
<td>33</td>
<td>15-30</td>
<td>Ressler 2006</td>
<td>4 KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td>034 01</td>
<td>34</td>
<td>1-9</td>
<td>Ressler 2006</td>
<td>4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>038 01</td>
<td>38</td>
<td>1-3</td>
<td>Ressler 2006</td>
<td>4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>038 04</td>
<td>38</td>
<td>4-23</td>
<td>Koelle et al 2006</td>
<td>2 (internet version) Verschleierung</td>
</tr>
<tr>
<td></td>
<td>038 27</td>
<td>38</td>
<td>27-30</td>
<td>Westphal and Blaxton 1998</td>
<td>201 KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td>039 01</td>
<td>39</td>
<td>1-20</td>
<td>Westphal and Blaxton 1998</td>
<td>201 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>040 01</td>
<td>40</td>
<td>1-9</td>
<td>Carley 2006</td>
<td>53 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>040 22</td>
<td>40</td>
<td>22-32</td>
<td>Ressler 2006</td>
<td>4, 5 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>041 01</td>
<td>41</td>
<td>1-6</td>
<td>Ressler 2006</td>
<td>6 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>041 08</td>
<td>41</td>
<td>8-15</td>
<td>Saxena et al. 2004</td>
<td>85 Verschleierung</td>
</tr>
<tr>
<td></td>
<td>041 28</td>
<td>41</td>
<td>28-31</td>
<td>Visualcomplexity 2006</td>
<td>1 Verschleierung</td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZeileArbeit</td>
<td>Quelle</td>
<td>SeiteQuelle</td>
<td>Typus</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------------------------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Nm/Fragment 042 01</td>
<td>42</td>
<td>1-2</td>
<td>Visualcomplexity 2006</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 042 03</td>
<td>42</td>
<td>3-9</td>
<td>TrackingTheThreat.com 2006</td>
<td>1</td>
<td>(internet version) Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 042 12</td>
<td>42</td>
<td>12-18</td>
<td>Saxena et al. 2004</td>
<td>85</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 044 18</td>
<td>44</td>
<td>18-22</td>
<td>Ressler 2006</td>
<td>6</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 044 23</td>
<td>44</td>
<td>23-30</td>
<td>Hamill_2006</td>
<td>3</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 045 01</td>
<td>45</td>
<td>1-16</td>
<td>Carley 2006</td>
<td>51-52</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 045 18</td>
<td>45</td>
<td>18-23</td>
<td>Koschade 2005</td>
<td>2 and 3</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 046 09</td>
<td>46</td>
<td>9-19</td>
<td>Hamill_2006</td>
<td>9</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 047 09</td>
<td>47</td>
<td>9-15</td>
<td>Hamill 2006</td>
<td>11</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 047 22</td>
<td>47</td>
<td>22-25</td>
<td>Hamill 2006</td>
<td>11</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 048 05</td>
<td>48</td>
<td>5-6</td>
<td>Hamill 2006</td>
<td>11</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 049 04</td>
<td>49</td>
<td>3-28</td>
<td>DCSINT_2005</td>
<td>2-10</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 050 01</td>
<td>50</td>
<td>1-21</td>
<td>DCSINT_2005</td>
<td>2-10</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 050 22</td>
<td>50</td>
<td>22-30</td>
<td>Bedi 2005</td>
<td>6</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 051 01</td>
<td>51</td>
<td>1-2, 4-31</td>
<td>Bedi 2005</td>
<td>6-7</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 052 01</td>
<td>52</td>
<td>1-17</td>
<td>Bedi 2005</td>
<td>7</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 052 18</td>
<td>52</td>
<td>18-29</td>
<td>Shelley 2002</td>
<td>1</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 053 01</td>
<td>53</td>
<td>1-20</td>
<td>Shelley 2002</td>
<td>1 (internet version)</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 053 21</td>
<td>53</td>
<td>21-30</td>
<td>Shelley 2002</td>
<td>2 (internet version)</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 054 01</td>
<td>54</td>
<td>1-12</td>
<td>Shelley 2002</td>
<td>2 (internet version)</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 054 13</td>
<td>54</td>
<td>13-23</td>
<td>Shelley 2002</td>
<td>4 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 054 23</td>
<td>54</td>
<td>23-32</td>
<td>Shelley 2002</td>
<td>4 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 055 01</td>
<td>55</td>
<td>1-7</td>
<td>Shelley 2002</td>
<td>4 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 057 11</td>
<td>57</td>
<td>11-29</td>
<td>terrorism_research_2005</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 058 01</td>
<td>58</td>
<td>1-30</td>
<td>DCSINT_2005</td>
<td>3-1, 3-2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 059 01</td>
<td>59</td>
<td>1-10</td>
<td>DCSINT_2005</td>
<td>3-2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 059 11</td>
<td>59</td>
<td>11-18</td>
<td>DCSINT_2005</td>
<td>3-2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 060 01</td>
<td>60</td>
<td>1-4</td>
<td>DCSINT_2005</td>
<td>3-2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 060 05</td>
<td>60</td>
<td>5-9</td>
<td>DCSINT_2005</td>
<td>3-2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 060 10</td>
<td>60</td>
<td>10-32</td>
<td>DCSINT_2005</td>
<td>3-2, 3-3</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZeileArbeit</td>
<td>Quelle</td>
<td>SeiteQuelle</td>
<td>Typus</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>061 01</td>
<td>61</td>
<td>1-13</td>
<td>DCSINT_2005</td>
<td>3-3 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>061 14</td>
<td>61</td>
<td>14-30</td>
<td>DCSINT_2005</td>
<td>3-4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>062 01</td>
<td>62</td>
<td>1-16</td>
<td>DCSINT_2005</td>
<td>3-4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>062 17</td>
<td>62</td>
<td>17-29</td>
<td>DCSINT_2005</td>
<td>3-4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>063 01</td>
<td>63</td>
<td>1-29</td>
<td>DCSINT_2005</td>
<td>3-4, 3-5 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>064 01</td>
<td>64</td>
<td>1</td>
<td>DCSINT_2005</td>
<td>3-5 KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>064 02</td>
<td>64</td>
<td>2-16</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>69 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>065 01</td>
<td>65</td>
<td>1-33</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>69, 70 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>066 01</td>
<td>66</td>
<td>1-33</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>70, 71 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>067 02</td>
<td>67</td>
<td>2-32</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>71 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>068 01</td>
<td>68</td>
<td>1-17</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>71-72 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>068 18</td>
<td>68</td>
<td>18-30</td>
<td>DCSINT_2005</td>
<td>2-12 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>069 01</td>
<td>69</td>
<td>1-6</td>
<td>DCSINT_2005</td>
<td>2-12 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>069 06</td>
<td>69</td>
<td>6-11</td>
<td>Lemieux_2003</td>
<td>5 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>069 12</td>
<td>69</td>
<td>12-30</td>
<td>DCSINT_2005</td>
<td>2-12, 2-13 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>070 01</td>
<td>70</td>
<td>1-32</td>
<td>DCSINT_2005</td>
<td>2-13 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>071 01</td>
<td>71</td>
<td>1-16</td>
<td>DCSINT_2005</td>
<td>2-13, 2-14 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>071 17</td>
<td>71</td>
<td>17-32</td>
<td>DCSINT_2005</td>
<td>2-14 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>072 01</td>
<td>72</td>
<td>1-26</td>
<td>DCSINT_2005</td>
<td>2-14, 2-15 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>072 27</td>
<td>72</td>
<td>27-32</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>72 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>073 01</td>
<td>73</td>
<td>1-31</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>72-73 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>074 01</td>
<td>74</td>
<td>1-7</td>
<td>Arquilla_Ronfeldt_2001</td>
<td>73 KomplettPlagiat</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>074 08</td>
<td>74</td>
<td>8-30</td>
<td>Lemieux_2003</td>
<td>6, 12 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>075 07</td>
<td>75</td>
<td>7-25</td>
<td>Xu and Chen 2005a</td>
<td>102 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>076 01</td>
<td>76</td>
<td>1-17, 20-25, 29-32</td>
<td>Xu and Chen 2005a</td>
<td>102 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>077 03</td>
<td>77</td>
<td>3-29</td>
<td>Xu and Chen 2005a</td>
<td>103 BauernOpfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>078 01</td>
<td>78</td>
<td>1-13</td>
<td>Xu and Chen 2005a</td>
<td>103 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>079 03</td>
<td>79</td>
<td>3-18</td>
<td>Xu etal 2004</td>
<td>3 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>079 19</td>
<td>79</td>
<td>19-29</td>
<td>Clark etal 2005</td>
<td>4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>080 01</td>
<td>80</td>
<td>1-29</td>
<td>Xu etal 2004</td>
<td>3-4 Verschleierung</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZelleArbeit</td>
<td>Quelle</td>
<td>SeiteQuelle</td>
<td>Typus</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Nm/Fragment 081 01</td>
<td>81</td>
<td>1-32</td>
<td>Xu etal 2004</td>
<td>5</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 082 01</td>
<td>82</td>
<td>1-32</td>
<td>Xu etal 2004</td>
<td>5, 6</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 083 01</td>
<td>83</td>
<td>1-3</td>
<td>Xu_etal_2004</td>
<td>6</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 083 04</td>
<td>83</td>
<td>4-30</td>
<td>CNS_2002</td>
<td>80, 95, 172</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 084 01</td>
<td>84</td>
<td>1-10</td>
<td>CNS_2002</td>
<td>172</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 084 11</td>
<td>84</td>
<td>11-33</td>
<td>Berry_etal_2004</td>
<td>1, 2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 085 01</td>
<td>85</td>
<td>1-7</td>
<td>Berry_etal_2004</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 085 08</td>
<td>85</td>
<td>8-27</td>
<td>Clauset_Young_2005</td>
<td>5</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 085 28</td>
<td>85</td>
<td>28-32</td>
<td>Xu etal 2004</td>
<td>6</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 086 01</td>
<td>86</td>
<td>1-15</td>
<td>Xu etal 2004</td>
<td>6-7</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 086 25</td>
<td>86</td>
<td>25-32</td>
<td>Xu etal 2004</td>
<td>7</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 087 01</td>
<td>87</td>
<td>1-11</td>
<td>Xu etal 2004</td>
<td>7, 8</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 087 12</td>
<td>87</td>
<td>12-32</td>
<td>CNS_2002</td>
<td>18, 105</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 088 01</td>
<td>88</td>
<td>1-20</td>
<td>CNS_2002</td>
<td>18, 105</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 088 21</td>
<td>88</td>
<td>21-33</td>
<td>Dombroski Carley 2002</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 089 01</td>
<td>89</td>
<td>1-2</td>
<td>Dombroski Carley 2002</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 089 03</td>
<td>89</td>
<td>3-25</td>
<td>CNS_2002</td>
<td>14, 18, 20</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 090 13</td>
<td>90</td>
<td>13-24</td>
<td>Xu etal 2004</td>
<td>8, 10</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 091 11</td>
<td>91</td>
<td>11-20</td>
<td>Ressler 2006</td>
<td>4</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 091 21</td>
<td>91</td>
<td>21-28</td>
<td>Ressler 2006</td>
<td>4, 5</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 093 04</td>
<td>93</td>
<td>4-16</td>
<td>Xu_and_Ch_2003</td>
<td>232</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 093 17</td>
<td>93</td>
<td>17-25</td>
<td>Katz et al 2004</td>
<td>308</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 094 01</td>
<td>94</td>
<td>1-25</td>
<td>Katz et al 2004</td>
<td>308-309</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 094 28</td>
<td>94</td>
<td>28-32</td>
<td>Xu and Chen 2003</td>
<td>232</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 095 01</td>
<td>95</td>
<td>1-8</td>
<td>Xu and Chen 2003</td>
<td>233</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 095 12</td>
<td>95</td>
<td>12-15</td>
<td>Borgatti_2002</td>
<td>1</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 096 02</td>
<td>96</td>
<td>2-20</td>
<td>Borgatti_2002</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 097 01</td>
<td>97</td>
<td>1-8</td>
<td>Borgatti_2002</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 097 09</td>
<td>97</td>
<td>9-19</td>
<td>Brandes_Erlebach_2005</td>
<td>7, 8</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 098 09</td>
<td>98</td>
<td>9-22</td>
<td>Borgatti_2002</td>
<td>3</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZeileArbeit</td>
<td>Quelle</td>
<td>SeiteQuelle</td>
<td>Typus</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------------------------------------------</td>
<td>-------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>099 01</td>
<td>1-25</td>
<td>Borgatti_2002</td>
<td>3-4</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>099 26</td>
<td>26-32</td>
<td>Brandes_Erlebach_2005</td>
<td>8</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>100 01</td>
<td>1-16</td>
<td>Brandes_Erlebach_2005</td>
<td>8, 9</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>100 24</td>
<td>24-30</td>
<td>Stephenson and Zelen 1989</td>
<td>2-3</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>101 01</td>
<td>1-8</td>
<td>Scott_1987</td>
<td>23</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>101 20</td>
<td>20-26</td>
<td>Koschuetzki_etal_2005</td>
<td>20</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>102 02</td>
<td>2-28</td>
<td>Scott_1987</td>
<td>83-85</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>103 15</td>
<td>15-27</td>
<td>Koschuetzki_etal_2005</td>
<td>22-23</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>104 02</td>
<td>2-8</td>
<td>Stephenson and Zelen 1989</td>
<td>3</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>104 12</td>
<td>12-24</td>
<td>Koschuetzki_etal_2005</td>
<td>29-30</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>106 14</td>
<td>14-17</td>
<td>Balasundaram et al 2006</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>107 01</td>
<td>1-4</td>
<td>Balasundaram et al 2006</td>
<td>2</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>107 07</td>
<td>7-23</td>
<td>Penzar_etal_2005</td>
<td>33-34</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>108 02</td>
<td>2-19</td>
<td>Penzar_etal_2005</td>
<td>34</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>109 01</td>
<td>1-13</td>
<td>Penzar_etal_2005</td>
<td>34, 35</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>111 17</td>
<td>17-27</td>
<td>Holmgren 2006</td>
<td>956</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>112 01</td>
<td>1-27</td>
<td>Holmgren 2006</td>
<td>956-957</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>113 01</td>
<td>1-22</td>
<td>Holmgren 2006</td>
<td>957</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>113 23</td>
<td>23-27</td>
<td>Chen 2006</td>
<td>98</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>114 01</td>
<td>1-12</td>
<td>Chen 2006</td>
<td>98-99</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>114 13</td>
<td>13-19</td>
<td>Chen 2006</td>
<td>98</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>114 20</td>
<td>20-33</td>
<td>Krebs 2004</td>
<td>1 (internet version)</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>115 01</td>
<td>1-3</td>
<td>Krebs 2004</td>
<td>1 (internet version)</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>115 04</td>
<td>4-10</td>
<td>Chen 2006</td>
<td>99-100</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>115 12</td>
<td>12-23</td>
<td>Qin et al 2005</td>
<td>299</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>117 01</td>
<td>1-2, 3-8</td>
<td>Chen 2006</td>
<td>98</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>118 08</td>
<td>8, 12-25</td>
<td>Latora and Marchiori 2004</td>
<td>70</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>125 01</td>
<td>1-29</td>
<td>Wikipedia_Riyadh_compound_bombings_2007</td>
<td>1 (internet version)</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>126 01</td>
<td>1-10</td>
<td>Wikipedia_Riyadh_compound_bombings_2007</td>
<td>1 (internet version)</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment</td>
<td>138 12</td>
<td>12-20</td>
<td>Freeman 1980</td>
<td>587</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZelleArbeit</td>
<td>Quelle</td>
<td>SeiteQuelle</td>
<td>Typus</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------------------------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Nm/Fragment 139 11</td>
<td>139</td>
<td>11-14</td>
<td>Freeman 1980</td>
<td>588</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 140 01</td>
<td>140</td>
<td>1-6</td>
<td>Freeman 1980</td>
<td>588</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 143 02</td>
<td>143</td>
<td>2-5</td>
<td>Stephenson and Zelen 1989</td>
<td>26-27</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 144 13</td>
<td>144</td>
<td>13-15</td>
<td>Stephenson and Zelen 1989</td>
<td>27</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 144 16</td>
<td>144</td>
<td>16-21</td>
<td>Stephenson and Zelen 1989</td>
<td>3</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 146 03</td>
<td>146</td>
<td>3-15</td>
<td>Penzar_etal_2005</td>
<td>28</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 146 20</td>
<td>146</td>
<td>20-25</td>
<td>Combating Terrorism Center 2006</td>
<td>8</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 147 01</td>
<td>147</td>
<td>1-13</td>
<td>Combating Terrorism Center 2006</td>
<td>8</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 147 18</td>
<td>147</td>
<td>18-29</td>
<td>Yang_etal_2005</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 162 03</td>
<td>162</td>
<td>3-8</td>
<td>Krebs 2002</td>
<td>46</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 165 01</td>
<td>165</td>
<td>1, 3-6</td>
<td>Latora and Marchiori 2004</td>
<td>73</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 166 11</td>
<td>166</td>
<td>11-18</td>
<td>WorldNetDaily - Wheeler 2003</td>
<td>1</td>
<td>(internet version) KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 168 03</td>
<td>168</td>
<td>3-13</td>
<td>Wikipedia - Adnan Gulshair el Shukrijumah - 2006</td>
<td>1 (internet version) KomplettPlagiat</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 169 01</td>
<td>169</td>
<td>1-10</td>
<td>Wikipedia - Adnan Gulshair el Shukrijumah - 2006</td>
<td>1 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 170 02</td>
<td>170</td>
<td>2-7</td>
<td>Wikipedia - World Trade Center bombing (1993) - 2006</td>
<td>1 (internet version) BauernOpfer</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 171 01</td>
<td>171</td>
<td>1-4</td>
<td>Wikipedia - World Trade Center bombing (1993) - 2006</td>
<td>1 (internet version) BauernOpfer</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 174 02</td>
<td>174</td>
<td>2-16</td>
<td>Wikipedia-Bojinka-plot_2006</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 178 05</td>
<td>178</td>
<td>5-15</td>
<td>Perer_Shneiderman_2006</td>
<td>693</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 180 02</td>
<td>180</td>
<td>2-16</td>
<td>Perer_Shneiderman_2006</td>
<td>693</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 181 01</td>
<td>181</td>
<td>1-33</td>
<td>Perer_Shneiderman_2006</td>
<td>693</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 182 01</td>
<td>182</td>
<td>1-33</td>
<td>Perer_Shneiderman_2006</td>
<td>694</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 183 01</td>
<td>183</td>
<td>1-14</td>
<td>Perer_Shneiderman_2006</td>
<td>694</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 183 17</td>
<td>183</td>
<td>17-24</td>
<td>Heer et al 2005</td>
<td>1 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 183 25</td>
<td>183</td>
<td>25-28</td>
<td>Heer et al 2005</td>
<td>3 (internet version) BauernOpfer</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 184 09</td>
<td>184</td>
<td>9-11, 12-15</td>
<td>Heer et al 2005</td>
<td>3 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 185 01</td>
<td>185</td>
<td>1-27</td>
<td>Heer et al 2005</td>
<td>3-4 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 186 03</td>
<td>186</td>
<td>3-32</td>
<td>Heer et al 2005</td>
<td>4</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 187 01</td>
<td>187</td>
<td>1-31</td>
<td>Heer et al 2005</td>
<td>4-5 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 188 01</td>
<td>188</td>
<td>1-30</td>
<td>Heer et al 2005</td>
<td>5 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Nm/Fragment 189 01</td>
<td>189</td>
<td>1-29</td>
<td>Heer et al 2005</td>
<td>5 (internet version) Verschleierung</td>
<td></td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZeileArbeit</td>
<td>Quelle</td>
<td>SeiteQuelle</td>
<td>Typus</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------------------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Nm/Fragment 190 03</td>
<td>190</td>
<td>3-16</td>
<td>Heer et al 2005</td>
<td>5 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 190 17</td>
<td>190</td>
<td>17-31</td>
<td>Heer et al 2005</td>
<td>9 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 191 01</td>
<td>191</td>
<td>1-6</td>
<td>Heer et al 2005</td>
<td>10 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 191 10</td>
<td>191</td>
<td>10-19</td>
<td>Xu and Chen 2005a</td>
<td>104-105</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 191 20</td>
<td>191</td>
<td>20-25</td>
<td>Xu and Chen 2005a</td>
<td>106</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 192 01</td>
<td>192</td>
<td>1-12</td>
<td>Smith and King 2002</td>
<td>5 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 193 01</td>
<td>193</td>
<td>1-12</td>
<td>Smith and King 2002</td>
<td>6 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 194 01</td>
<td>194</td>
<td>1-7</td>
<td>Smith and King 2002</td>
<td>6 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 195 02</td>
<td>195</td>
<td>2-12</td>
<td>Smith and King 2002</td>
<td>7 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 198 03</td>
<td>198</td>
<td>3-18</td>
<td>Xu and Chen 2005b</td>
<td>201</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 199 10</td>
<td>199</td>
<td>10-15</td>
<td>Perer_Sheiderman_2006</td>
<td>693</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 199 27</td>
<td>199</td>
<td>27-28</td>
<td>Xu and Chen 2005a</td>
<td>106</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 200 01</td>
<td>200</td>
<td>1-4</td>
<td>Xu and Chen 2005a</td>
<td>106</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 202 12</td>
<td>202</td>
<td>12-21</td>
<td>Tsvetovat et al. 2005</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 205 21</td>
<td>205</td>
<td>21-23</td>
<td>Zhao et al 2006</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 206 01</td>
<td>206</td>
<td>1-21</td>
<td>Zhao et al 2006</td>
<td>2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 206 26</td>
<td>206</td>
<td>26-28</td>
<td>Jensen et al 2003</td>
<td>381</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 207 01</td>
<td>207</td>
<td>1-6</td>
<td>Jensen et al 2003</td>
<td>381</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 207 12</td>
<td>207</td>
<td>12-18, 20, 21-22,</td>
<td>Frost 1982</td>
<td>358</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 208 01</td>
<td>208</td>
<td>1-10</td>
<td>Frost 1982</td>
<td>359</td>
<td>BauernOpfer</td>
</tr>
<tr>
<td>Nm/Fragment 208 11</td>
<td>208</td>
<td>11-15, 17-18, 24-28,</td>
<td>Frost 1982</td>
<td>360-361</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 214 02</td>
<td>214</td>
<td>2-7</td>
<td>TrackingTheThreat.com 2006a</td>
<td>1 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 214 07</td>
<td>214</td>
<td>7-14</td>
<td>TrackingTheThreat.com 2006</td>
<td>1 (internet version)</td>
<td>KomplettPlagiat</td>
</tr>
<tr>
<td>Nm/Fragment 214 15</td>
<td>214</td>
<td>15-24</td>
<td>TrackingTheThreat.com 2006</td>
<td>1 (internet version)</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 215 01</td>
<td>215</td>
<td>1-4</td>
<td>Dugan_etal_2006</td>
<td>409</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 215 11</td>
<td>215</td>
<td>11-31</td>
<td>Malin_etal_2005</td>
<td>119, 120</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 216 05</td>
<td>216</td>
<td>5-30</td>
<td>Dugan_etal_2006</td>
<td>410-411</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 219 04</td>
<td>219</td>
<td>4-8, 10-23, 24-26,</td>
<td>Balasundaram et al 2006</td>
<td>1, 2</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 219 27</td>
<td>219</td>
<td>27-28</td>
<td>Stokman_2004</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Nm/Fragment 220 01</td>
<td>220</td>
<td>1-14</td>
<td>Stokman_2004</td>
<td>1</td>
<td>Verschleierung</td>
</tr>
<tr>
<td>Fragment</td>
<td>SeiteArbeit</td>
<td>ZeileArbeit</td>
<td>Quelle</td>
<td>Seite</td>
<td>Quelle</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>Nm/Fragment 220 14</td>
<td>220</td>
<td>14-29</td>
<td>Aviv et al 2003</td>
<td>4</td>
<td>Aviv et al 2003</td>
</tr>
<tr>
<td>Nm/Fragment 221 23</td>
<td>221</td>
<td>23-29</td>
<td>Balasundaram et al 2006</td>
<td>2</td>
<td>Balasundaram et al 2006</td>
</tr>
<tr>
<td>Nm/Fragment 222 01</td>
<td>222</td>
<td>1-25</td>
<td>Balasundaram et al 2006</td>
<td>2</td>
<td>Balasundaram et al 2006</td>
</tr>
<tr>
<td>Nm/Fragment 231 10</td>
<td>231</td>
<td>10-14</td>
<td>Aviv et al 2003</td>
<td>10</td>
<td>Aviv et al 2003</td>
</tr>
<tr>
<td>Nm/Fragment 239 10</td>
<td>239</td>
<td>10-20</td>
<td>Hamill_2006</td>
<td>278</td>
<td>Hamill_2006</td>
</tr>
<tr>
<td>Nm/Fragment 240 24</td>
<td>240</td>
<td>24-26</td>
<td>Hamill_2006</td>
<td>278</td>
<td>Hamill_2006</td>
</tr>
<tr>
<td>Nm/Fragment 241 01</td>
<td>241</td>
<td>1-3</td>
<td>Hamill 2006</td>
<td>278</td>
<td>Hamill 2006</td>
</tr>
<tr>
<td>Nm/Fragment 242 09</td>
<td>242</td>
<td>9-14</td>
<td>Stephenson and Zelen 1989</td>
<td>3</td>
<td>Stephenson and Zelen 1989</td>
</tr>
<tr>
<td>Nm/Fragment 243 23</td>
<td>243</td>
<td>23-26</td>
<td>Saxena et al. 2004</td>
<td>94</td>
<td>Saxena et al. 2004</td>
</tr>
<tr>
<td>Nm/Fragment 244 21</td>
<td>244</td>
<td>21-32</td>
<td>Ressler 2006</td>
<td>7</td>
<td>Ressler 2006</td>
</tr>
<tr>
<td>Nm/Fragment 245 01</td>
<td>245</td>
<td>1-5</td>
<td>Ressler 2006</td>
<td>7</td>
<td>Ressler 2006</td>
</tr>
<tr>
<td>Nm/Fragment 246 08</td>
<td>246</td>
<td>8-28</td>
<td>Lemieux_2003</td>
<td>12-13</td>
<td>Lemieux_2003</td>
</tr>
<tr>
<td>Nm/Fragment 247 01</td>
<td>247</td>
<td>1-21</td>
<td>Lemieux_2003</td>
<td>13</td>
<td>Lemieux_2003</td>
</tr>
<tr>
<td>Nm/Fragment 247 22</td>
<td>247</td>
<td>22-29</td>
<td>Ressler 2006</td>
<td>7-8</td>
<td>Ressler 2006</td>
</tr>
<tr>
<td>Nm/Fragment 248 01</td>
<td>248</td>
<td>1-9</td>
<td>Ressler 2006</td>
<td>8</td>
<td>Ressler 2006</td>
</tr>
<tr>
<td>Nm/Fragment 248 24</td>
<td>248</td>
<td>24-28</td>
<td>Hamill_2006</td>
<td>285</td>
<td>Hamill_2006</td>
</tr>
<tr>
<td>Nm/Fragment 249 01</td>
<td>249</td>
<td>1-8</td>
<td>Hamill_2006</td>
<td>285</td>
<td>Hamill_2006</td>
</tr>
</tbody>
</table>

**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**
I. INTRODUCTION

1.1. OVERVIEW

Terrorists seldom operate in a 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 a network consisting of nodes for example, terrorists, terrorist camps, supporting countries, etc.) and links (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.

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 a 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).]
For example, two terrorists might have a formal tie (one is a 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 distinguishes 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 (Attē attends meeting with Nawaf Alhażmi) or differ in direction (Bin Laden gives advice to Attē vs. Attē gets advice from Bin Laden). They may differ in content (Attē 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, e-mail, 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).

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

Untersuchte Arbeit:
Seite: 21, Zeilen: 1-5

[For example, arrest of central members in a network may affect the operation of 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).]

Quelle: Xu and Chen 2003
Seite(n): 233, Zeilen: 1-4

[For example, 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].]

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.

Farbig

Untersuchte Arbeit:
Seite: 23, Zeilen: 27-30

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).

Quelle: DeRosa 2004
Seite(n): v, Zeilen: 2-5

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.

Anmerkungen

Although the source is given nothing is marked as a citation.
**Untersuchte Arbeit: BauernOpfer**

**Seite: 24, Zeilen: 4-20**

*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 behavior, 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.

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.

**Quelle: DeRosa 2004**

**Seite(n): v, Zeilen: 19-25, 32-38**

"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 discover 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 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.

**Anmerkungen**

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

---

**Untersuchte Arbeit: Verschleierung**

**Seite: 25, Zeilen: 22-29**

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).

**Quelle: Koschade_2005**

**Seite(n): 2, 3, Zeilen: p2:6-8; p3:31-35**

Social network analysis offers the ability to firstly map a covert cell, and to secondly measure the specific structural and interactive criteria of such a cell. 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]


**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.
This technique is also known as subject based link analysis. This technique uses aggregated public records or other large collections 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.

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.

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]

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.

Anmerkungen
no source given

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.

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.

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).

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).

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

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

A hindsight analysis of the September 11 attacks provides an example of how simple, subject-based link analysis could have been used 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.
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:

**Watch List Information (Direct Links)**
- 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. They 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)**
- Muhammad Atta and Mavan Al shehhi, both hijackers used the same contact address for their flight reservations that Khalid Almihdhar used for his flight reservation.
- Salem Alhazmi, used the same contact address on his reservation as Nawaf Alhazmi.
- Majed Moqed used the same frequent flyer number that Khalid Almihdhar used in his reservation.
- Hamza Alghamdi, used the same contact address on his reservation as Ahmed Alghamdi used in his reservation.
- Hani Hanjour, lived with both Nawaf Alhazmi and Khalid Almihdhar, a fact that searches of public records could have revealed.

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.

**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.

**Anmerkungen**

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

**Untersuchte Arbeit:**
Seite: 31, Zeilen: 15-27

"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.

Anmerkungen

Taken from a textbook on data-mining without reference.

**Quelle:** Han_Kamber_2006

"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 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.

Anmerkungen

Taken from a textbook on data-mining without reference.

**[18.] Nm/Fragment 032 02**

**Verschleierung**

**Untersuchte Arbeit:**
Seite: 32, Zeilen: 2-10

(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.

Anmerkungen

Taken from a textbook on data-mining without reference.

**Quelle:** Han_Kamber_2006
Seite(n): 561, 562, Zeilen: -

[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.
1.5. LIMITATIONS

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.

1.5.1 Issues in Data Collection

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 ties 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.

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.

Anmerkungen

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

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 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.
Understanding Terror Networks by Marc Sageman was another brilliant attempt in this regard. He used 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.

Anmerkungen
Continued from previous page.

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.

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

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 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 theoretic algorithms do not typically consider attributes on links or nodes.

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

Keine Kennzeichnung als Zitat, kein Hinweis auf die Quelle

Verschleierung

Verschleierung

KomplettPlagiat

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.]

Anmerkungen

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

Quelle: Westphal and Blaxton 1998

Seite(n): 201, Zeilen: 1-20

[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 forms 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.

Anmerkungen

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

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 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 […]

Anmerkungen

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

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. 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.

There has been limited work in the field of complex modeling of terrorist networks outside the work of Kathleen Carley and her associates.

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. [...]

Continued from last page: no reference to the source is given.
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 new ways by providing huge volume of information on these incidents. Such information in open domain can be used to create a knowledge base which, after proper cleaning could be useful for intelligence analysis.

Anmerkungen
The source is not mentioned in the entire thesis.

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.

Anmerkungen
the source is not given

[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.

Anmerkungen
Source is not given. Copied text starts on the previous page.
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 open-source 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.

Anmerkungen
not marked as a citation, no source given

Terrorist and criminal organizations, generally organize themselves as secret networks with distributed work share. It is difficult to obtain confirmed information in the open domain on their membership, ties 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.

Anmerkungen
No source is given for this short paragraph.

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.

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.
### 1.8. PROBLEM DEFINITION

The primary objective of this research is to expand data mining research, sociological, and behavioral 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).

**Anmerkungen**

The original source Hamill (2006) is not given.

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

### 1.2 Problem Definition

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].

---

### Other fragments

**Terrorist networks are so often challenging to reason about and manage.**...
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”.

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.

This framework aims to connect the dots between individuals and “map and measure complex, sometimes 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”.

---


The primary objective of this research is to develop the underlying theory and associated methodology used to produce and analyze terrorist networks and proposes mathematical methods for destabilizing these adversaries. The specific objectives of this research include:

- 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.

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.
• 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 [...] 

Anmerkungen

no source given, nothing marked as a citation

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.

Anmerkungen

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

Chapter 9 provides an overall, general conclusions as well as recommendations for future research.

Anmerkungen

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

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


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.

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’"

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.

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.
[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.

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.

4) Known hard-core terrorists: People on the most wanted list of the FBI and other intelligence or law enforcement agencies.

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.]
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 any database.

The third category of terrorists are for example, the Madrid bombers who may not have been on the US OFAC 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 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.

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.

---

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).

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 central threats to our national and international security. Yet, more needs to be understood about the inter-linkage between the two phenomena.

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.
<table>
<thead>
<tr>
<th>Untersuchte Arbeit:</th>
<th>Quelle: Shelley 2002</th>
</tr>
</thead>
</table>

BauernOpfer

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 support themselves financially.
2) Organized crime groups and terrorists 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 areas with little governmental controls, weak enforcement of laws and open borders.
4) Both organized criminals and terrorists corrupt local officials to achieve their objectives.
5) Organized crime groups and terrorists use similar methods and operators to move their funds.
6) Organized crime groups and terrorists 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.

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.

Anmerkungen

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

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 to communicate. The communication is facilitated with encryption and steganography (hiding messages within other messages). They are non-state actors striking at the citizens of a state or different states.
Members of a terrorist group are given special training on 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.]

Anmerkungen
still copying from Shelley (2002)

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.

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

Anmerkungen

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

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.

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.

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 ("bottom-up" instead of "top-down").

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.
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.

Anmerkungen
this finishes the list - still no mention of the source

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.]

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

Some groups will also use coercion and leverage to gain limited or one-time cooperation from useful individuals. This cooperation can range anywhere like gaining information to conducting a suicide bombing operation. 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.

[FIGURE]

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 keep activists out of jail and free to continue conducting actions.
Operating in cells not only guarantees the security of group members but also such decentralized structure helps 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.

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.

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.

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.

2.7 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.

Anmerkungen

Text nearly identical, but the source is not mentioned.

2.7.2 Netzwerkstruktur

Terroristen sind in dieser Dekade zunehmend ein Teil einer viel weiteren und breiteren Netzwerklandschaft als es früher der Fall war. Gruppen, die auf religiöse oder einseitige Motive basieren, haben oft keine spezifische politische oder patriotische Agenda; diese Organisationen haben in der Regel weniger die Notwendigkeit einer hierarchischen Struktur. Stattdessen können sie auf lockerer Zuordnung mit ähnlichen Gruppen oder Einzelpersonen aus unterschiedlichen Orten zurückgreifen. Allgemeine Ziele und Ziele werden angekündigt, und die Einheiten und Initiativen sind an die Einzelpersonen oder Zellen. 

Anmerkungen

Die Quelle wird nicht erwähnt.
2.8 DIMENSIONS OF CRIMINAL/ TERRORIST 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 United States, 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.

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”).

Anmerkungen
Slight adaptations. The source is not given.
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 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].

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.
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.

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 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 fleeting relations 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.

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.]

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 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 short-term 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 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. 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.
Networks with their particular characteristics offer substantial eye-catching 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.

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.
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).

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.
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.


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 adjustments, but all content including four literature references can also be found in the source, which is not referenced.
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 terms and will, for example, mean completely different levels of income between Western Africa and Western Europe.

2.9.2 Education and Intellect

Generally Terrorists are educated to more than average level, except very few Western terrorists, which are uneducated or illiterate (Hudson, A. R, 1999).
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 communication and organizational 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.

2.9.3 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. [FN 121]

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.

Age

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 118] Ibid., 4.
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.

Terrorists are not exclusively male. Usually Women’s roles 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 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/lte).

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.
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 much less common in some right wing groups, particularly those with neo-Nazi and Christian Identity oriented ideologies.

### 2.9.5 Appearance

Terrorists 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 were a schoolteacher, 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, most terrorists do not marry, even though there have been cases of married couples within terrorist organizations.

---

**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.
### 2.9.6 Network Cores

Networks of any significant size will generally have a central core and a periphery, 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.

---

**Anmerkungen**

Slight adaptations. The source is not referenced.
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.

---

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.
### KomplettPlagiat

**Untersuchte Arbeit:**

Seite: 74, Zeilen: 1-7

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.

**Quelle:** Arquilla_Ronfeldt_2001

Seite(n): 73, Zeilen: 18ff

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 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".

---

### Verschleierung

**Untersuchte Arbeit:**

Seite: 74, Zeilen: 8-30

#### 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.]”

**Quelle:** Lemieux_2003

Seite(n): 6, 12, Zeilen: page 6: 1-2, 9-17 ; page 12: 2-5

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.

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.
**Verschleierung**

*Untersuchte Arbeit:*
*Seite: 75, Zeilen: 7-25*

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 from accidental data entry errors or from intentional cheating by criminals.

- **Inconsistency.** Information about criminals, who have captured a number of times at a number of places, may be entered into law enforcement databases multiple times.

**Quelle: Xu and Chen 2005a**
*Seite(n): 102, Zeilen: left column 53 - right column 1-21*

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.** Criminal networks are covert networks that operate in secrecy and stealth. 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.

- **Incorrectness.** Incorrect data regarding criminals' identities, physical characteristics, and addresses may result 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.

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.
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. The literature study found that the problems particularly 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. 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).

- **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).

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).
Criminal Network Analysis, which is a broad category of terrorist network analysis, can be categorized into three generations (Xu J., Chen H., 2006):

**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.

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.

**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 spreadsheet or text file.]

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 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).


Verschleierung

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 spreadsheet or text file.

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:

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.

For example, Analyst’s Notebook can automatically generate a link chart based on relational data from a spreadsheet or text file (Figure 2a).

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 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
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 structural 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.

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.

Anmerkungen

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

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.

Anmerkungen

No source given.
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 predictor of an individual's possible prosecution (Baker, W.E. and R.R. Faulkner 1993). Krebs analyzed 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, blockmodeling 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 study network dynamics. Doreian and Stokman classified existing approaches into three categories: descriptive, statistical, and simulation methods (Doreian, P. and F.N. Stokman, 1997).

In Proceedings of the 8th International Command and Control Research and Technology Symposium. Washington DC., VA.

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].


2.13.1 Descriptive methods

The descriptive analysis is often employed to detect structural changes in social networks. Descriptive 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.

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).

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.

Anmerkungen

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

Link stability has been researched in various case studies, especially inter-organizational network studies. 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).

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 sociomatrices 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).]

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.
Farbig

Untersuchte Arbeit:
Seite: 83, Zeilen: 1-3

[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);]

Anmerkungen

Continued from previous page

Verschleierung

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 quantify the stability or continuity of a scientific field as represented by a group of authors [2].


Farbig

Untersuchte Arbeit:
Seite: 83, Zeilen: 4-30

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.]


Anmerkungen

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

**Seite: 84, Zeilen: 1-10**

[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.](Abstract)

### Verschleierung

**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. 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.]
Farbig

Untersuchte Arbeit: Seite: 85, Zeilen: 1-7

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.

Anmerkungen

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

Farbig

Untersuchte Arbeit: Seite: 85, Zeilen: 8-27

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.

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.
### 2.13.2 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).

#### 3.1.2 Statistical Methods

**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].


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

[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 fit best with empirical data and 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 on the 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 of changing from one state to previous state, while the intensity matrix contains the transition rates (Hallinan, M.T., 1978/79; Leenders, R., 1997).

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 times. The 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 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].


Anmerkungen

Copied text starts on the previous page (Nm/Fragment_085_28). No source is given.
2.13.3 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.

Anmerkungen

No source given.

3.1.3 Simulation Methods

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 ability 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.

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 relationship with others affect the overall structure of a network (Hummon, N.P., 2000). 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.

Anmerkungen

No source given.
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.

**Anmerkungen**

No source given.

---

[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. 

**Anmerkungen**

No source given.
NETEST – Es basiert auf der Kombination von multi-agent technologie mit
hierarchischen Bayes-Inferrormodelle und biased net models to produce
accurate posterior network representations. Bayes-Inferrormodelle
produzieren Darstellungen einer Netzwerkstruktur und Informations-
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
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.]

Anmerkungen

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

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.

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.
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 straightforward methods (for example, Krebs V., 2002, Sageman, M., 2004) as described earlier.

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.

Nothing marked as a citation, no source named.
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

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 multiplex [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.
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 vary in sign, ranging from positive (Iraqis like Zarqawi) to negative (Jordanians dislike Zarqawi).

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 in understanding the organization, structure, and operation of criminal enterprises. Such knowledge can help law enforcement and intelligence agencies disrupt criminal networks and develop effective control strategies to combat organized crimes such as narcotic trafficking and terrorism.
For 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).


---

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.

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

The natural graphical representation of an adjacency matrix is a [table, such as shown in Figure 3.2.]

Anmerkungen
The source is not given. Note the slight adaptation to make the text fit the terrorist topic of the thesis.
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 stand for \( \{u, v\} \).

Graphs that can have directed as well undirected edges are called **mixed graphs**, but such graphs are encountered rarely.

### 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.

---

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 \( A \).

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.
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 \( v_0 = v_n \). A cycle can be defined as a closed path in which \( n \geq 3 \). 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 3.1, 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 \( v_0 = v_n \). A cycle can be defined as a closed path in which \( n \geq 3 \). 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.

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, e, 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 4. 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.

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., an edge whose end \( \text{vertices are identical} \), is called a loop.

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.
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 \( V' \subseteq V \) and \( E' \subseteq E \). 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 a 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 \( e \in E \).

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.

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 “degree”, “closeness”, and “betweenness”. His development is partially motivated by the structural properties of the center of a star graph.

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.
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 straightforward 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.

Anmerkungen
The source is not given here.

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.

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&dq=%22represent+a+static+situation+and+we+are+interested+in+the%22&source=bl&ots=0bA-of9GAw&sig=jYUZ9NhqErpmXxp5l4vXsfJYCM&hl=en&sa=X&ei=PWiWT9HTFYYnChAf9n8CADg&redir_esc=y#v=onepage&q=%22represent+a+static+situation+and+we+are+interested+in+the%22&f=false) and Memon, Hicks & Larsen (2007) (http://books.google.es/books?id=7URT9Xpfj4C&pg=PA436&dq=%22represent+a+static+situation+and+we+are+interested+in+the%22&source=bl&ots=ejgqP0nQn91sig=J8pXsfJ8C5Nd_eHTz3Ciz3WYic&hl=en&sa=X&ei=PWiWT9HTFYYnChAf9n8CADg&redir_esc=y#v=onepage&q=%22represent+a+static+situation+and+we+are+interested+in+the%22&f=false) . Henrik Legind Larsen is the thesis supervisor and David L. Hicks is the thesis committee chairman.
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 that 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.

Anmerkungen

Scott is mentioned in the thesis for the first time on page 220.
We denote the sum of the distances from a vertex \( u \in V \) to any other vertex in a graph \( G = (V, E) \) as the total distance
\[
\sum_{v \in V} d(u, v).
\]

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:

\[
C_C(u) = \frac{1}{\sum_{v \in V} d(u, v)}.
\]

\( C_C(u) \) 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 \( C_C(u) \) grows with decreasing total distance of \( u \) and it is clearly a structural index.

Anmerkungen

The source is not mentioned anywhere in the thesis.

---

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).

Anmerkungen

nothing is marked as a citation, the source remains unnamed.
Untersuchte Arbeit:
Seite: 104, Zeilen: 12-24

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

\[
C_B(v) = \sum_{s \neq v \in V} \sum_{t \neq v \in V} \delta_{st}(v) \quad (4)
\]

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.

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 \( \sigma_{st} \) 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

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

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].

Anmerkungen

To be continued on the next page Nm/Fragment_107_01
<table>
<thead>
<tr>
<th>Untersuchte Arbeit:</th>
<th>Quelle: Balasundaram et al 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seite: 107, Zeilen: 1-4</td>
<td>Seite(n): 2, Zeilen: 41-45</td>
</tr>
</tbody>
</table>

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.

Anmerkungen

The copied text starts on the previous page: Nm/Fragment_106_14
According to Kreb's (2002) analysis, this network had 62 members in total, of which 19 were kidnappers, 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.

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 other members on average, which means that average members are rather isolated from the rest of the network. The density 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.


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 chapter 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.
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, betweenness of forty nodes is in fact less than 1% and only six nodes have betweenness higher than 10%. These six 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).

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 chapter 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.
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 chapter 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.
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 Barabási, A.-L. (2002); Dorogovtsev, S. N., and Mendes, J. F. F. (2002); Newman, M. E. J. (2003)).

3.4.1 Degree Distribution

The degree \( k \) is the number of edges connecting to the \( i \)th 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.

Anmerkungen

Nearly identical, though the source is not mentioned anywhere.
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 these $k_i$ neighbors is $k_i(k_i-1)/2$. The clustering coefficient of $i^{th}$ vertex is defined as the ratio between the number 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 $C = (1/N) \sum_{i=1}^{n} C_i$.

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., $d = l$. 

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.
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 \textit{random graph} was introduced by Erdos and Renyi in the late 1950s and is one of the earliest theoretical models of a network (Bollobás, 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 \textit{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 \textit{scale-free network model}) that put the emphasis on how real networks evolve (Albert, R., Jeong, H., and Barabasi, A.-L., 2000).

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

[139.] Nm/Fragment 113 23

### Verschleierung

Three models have been used to distinguish complex networks: \textit{random graph model}, \textit{small-world model}, and \textit{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.

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.
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 self-organizing principle, where growth and preferential attachment play a key role for the emergence of the power law degree distribution (Chen, Hsinchun, 2006).

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).

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.
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.

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.

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).

Anmerkungen

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

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, [...]
### BauernOpfer

**Untersuchte Arbeit:**
Seite: 115, Zeilen: 12-23

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.

**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 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.

### Verschleierung

**Untersuchte Arbeit:**
Seite: 117, Zeilen: 1-2, 3-8

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.

**Quelle:** Chen 2006
Seite(n): 98, Zeilen: 29-33

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.
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 $C_{eff}$ in the interval of $[0, 1]$. 

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.
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", and it is reported as the terrible attack on Americans that year. In the attack, 35 people were killed, and over 160 injured.

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.

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 charge suddenly exploded as reported on the media, killing all of the terrorists 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.

---

[148.] Nm/Fragment 125 01

### Untersuchte Arbeit:

#### Seite: 125, Zeilen: 1-10

**3.7.2 Case 2: Riyadh Bombing Terrorists Network [FN 19]**

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", and the deadliest attack on Americans that year. Altogether, some 35 people were killed, and over 160 wounded.

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.

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 un-armed 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 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.

---

[149.] Nm/Fragment 126 01

### Untersuchte Arbeit:

#### Seite: 126, Zeilen: 1-10

[As] they fired roughly, they shouted phrases like "God is Great!". Then they exploded both of their bombs, destroying 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.

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 American citizens.

### 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.
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 nodes \( (u, v, w) \) 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.

**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).

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 […]

**Anmerkungen**

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

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.

**Anmerkungen**

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

We have proposed, developed and illustrated the use of examples a new measure of centrality called information, which may be applied to 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.

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.

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.
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 organisation”, extremely hard to destroy, especially by traditional anti-terrorist or counterterrorist methods.

### 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.
[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 Zubaydah, 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 mastermind 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).

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]


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.

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).

---

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."

---

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.

Anmerkungen

No reference given.
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 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.

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.

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 virtually 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 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.

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

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.

---


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

*Untersuchte Arbeit:*
Seite: 171, Zeilen: 1-4

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.

Seite(n): 1 (internet version), Zeilen: --

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.

---

**Verschleierung**

*Untersuchte Arbeit:*
Seite: 174, Zeilen: 2-16

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.

*Quelle: Wikipedia-Bojinka-plot_2006*
Seite(n): 1, Zeilen: 1ff

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.
### 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.

**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.
In practice, a network visualization of a domain can be a messy one, particularly when the network is very 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 detect interesting patterns in networks. Analysts might pursue a tight-knit community of the actors, or the brokers between them, or the most powerful actors – and there are many sophisticated algorithms for detecting these behaviors.

It is worthwhile to mention that more mature fields in the area known as biology have developed systematic methods to train beginners and guarantee uniformity among analysts. The techniques are complete, so if two analysts are able to present the same data, they most probably reach at the same conclusion. Though, in the social networks area, different networks need to be analyzed differently. The spread of an epidemic among small towns is not necessarily the same as a spread of a financial crisis on world markets (Watts D. J., 2003). From the above discussion, it is found that since there is no systematic way to interpret networks; researchers need to be able to flexibly explore patterns to discover patterns. 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 (Freeman L. C., 2004). 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. The book presents a review of network analysis methods and an overview of the field.


Numerous techniques try to use available display more proficiently by distorting the graph. 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, e.g. (Auber, et al., 2003; Parker G., 1998). Recent work associates these two techniques with fisheye views to decrease the number of displayed nodes while protecting the network structure (Gansner, E. R., 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. Batagell, 2005). The tools offer exciting techniques that users can perform 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.

Visualizations of social networks have been used to aid SNA from the beginning [EN 13]. The visualization of networks is more 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 in order to minimize link crossings and observe to visual principles. These 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).

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.


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.

[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.

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].


Although information visualization (infovis) techniques prove to be vital 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.

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.

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.

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).
6.3.3 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”. ItemRegistry 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.


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 perform tasks like filtering as described in previous subsections. Assignment actions set visual attributes, such as location, color, font, and size, for VisualItems. 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.

Anmerkungen

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

Renderers 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 renderers 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.

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.
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.


It also allows visual appearances to be easily changed, either by issuing different Renderers to respond 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 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. 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, grid-based, force-directed, top-down [EN 40], radial [EN 48]. indented outline, and tree map [EN 10, EN 44] algorithms.


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

**Verschleierung**

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

[Available layouts include random, circular, grid-based, 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, with 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 VisibleItems, 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

[Available layouts include random, circular, grid-based, forcedirected, 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 real-time 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 speed-dependent automatic zooming [EN 25].

---

**Anmerkungen**

continued from previous page.

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

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.

The prototype constructed in the research study using the Prefuse toolkit demonstrates the flexibility and performance of the Prefuse architecture.

Anmerkungen

continued from previous page

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

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.

Applications built with the toolkit demonstrate the flexibility and performance of the Prefuse architecture.
The 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.

Anmerkungen

continued from previous page;

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

6.4 SUBGROUP DETECTION

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.

The most of the material presented in this Section is already published in (Memon N., Larsen Henrik Legind, 2006c)

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.
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.

Anmerkungen

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

---

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 sub-graphs 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.

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].

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.
6.4.1.1 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 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. A user may specify the maximum length of a path from the object and the type of links that a connecting path 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.

6.4.1.2 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.

5.2.3 Retrieving all objects that are directly or indirectly connected to a specified object

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 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.

5.2.4 Finding paths that connect two specified objects

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.

Note how Nm adapts the text to make it suitable for the terrorism theme of the thesis: "Mary" becomes "Mars", 'Sandra' becomes "Saeen" and an "armed robbery" becomes a "bombing plot".
6.4.1.3 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 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.

5.2.5 Finding connections between groups of objects

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 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, [...

Anmerkungen

continued from previous page

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

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.

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.
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.

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

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.

Anmerkungen
no reference given
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.


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:

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.
Terrorist organizations such as Al Qaeda

Terrorists such as Osama Bin Ladin, Ramzi Yousef, etc.

Terrorist facilities such as Darunta Training Camp, Khalden Training Camp, etc.

Terrorist events/attacks such as 9/11, WTC terrorist attack 2003, 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.
- facilityOwner: instances of terrorist facility are usually run by instances of terrorist organizations.
- facilityMember: instances of terrorist are linked to various instances of terrorist facilities if the terrorist instance attended/spent some time at the facility.
- claimResponsibility: instances of terrorist organization are linked to the instances of terror attacks they claim responsibility for.
- participatedIn: instances of terrorist that may have participated in instances of terror attacks.

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.
- facilityOwner: instances of terrorist facility are usually run by instances of terrorist organizations.
- facilityMember: instances of terrorist are linked to various instances of terrorist facilities if the terrorist instance attended/spent some time at the facility.
- claimResponsibility: instances of terrorist organization are linked to the instances of terror attacks they claim responsibility for.
- participatedIn: instances of terrorist that may have participated in instances of terror attacks.

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").
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.]

---


Anmerkungen

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

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.

---

A simple 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 of all that terrorists met at Malaysia before 9/11" are met by issuing a simple retrieval call (terrorist, met at Malaysia before 9/11, ?) which delivers only that data which has been requested.

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.
It is to be noted that multi-attribute retrieval may be inefficient. The 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 of retrieving 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 a 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.

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]: retrieving the names of all 18 year old unemployed actresses with experience in movie-acting, 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.

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.

Anmerkungen

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

A barely concealed copy of the original text.

Anmerkungen

an almost literal copy, not marked as a citation

The source is not mentioned anywhere in the thesis.
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 exist 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.

Anmerkungen

The source is not mentioned anywhere in the thesis.
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.

Anmerkungen

The text has been copied with only slight adaptations, the source is not mentioned in the thesis anywhere.
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 worth to mention that SNA concepts provide suitable data mining tools for this purpose (Davis, R.H., 1981).

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.

Anmerkungen

The source is not given. The text is copied including all literature references. Only minor adjustments have been made.
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 micro-macro-macro link, the way in which individual behavior and collective phenomena are linked with one another. In this sense, social networks can assist the analysts both the root cause and the result of the behavior 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".

Anmerkungen

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

SNA methods provide specific mathematical definitions of five groups of characteristics of the actors 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 the 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)

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.
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.

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 k-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.

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).
<table>
<thead>
<tr>
<th>Fragment</th>
<th>Seite</th>
<th>Zeilen</th>
<th>Quelle</th>
<th>Seite(n)</th>
<th>Zeilen</th>
</tr>
</thead>
<tbody>
<tr>
<td>231 10</td>
<td>231</td>
<td>10-14</td>
<td>Aviv et al 2003</td>
<td>10</td>
<td>5-8</td>
</tr>
<tr>
<td>239 10</td>
<td>239</td>
<td>10-20</td>
<td>Hamill 2006</td>
<td>278</td>
<td>7-14</td>
</tr>
<tr>
<td>240 24</td>
<td>240</td>
<td>24-26</td>
<td>Hamill 2006</td>
<td>278</td>
<td>20-23</td>
</tr>
</tbody>
</table>

### KomplettPlagiat

**Untersuchte Arbeit:**
Seite: 231, Zeilen: 10-14

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.

**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 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].

**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.

### Verschleierung

**Untersuchte Arbeit:**
Seite: 239, Zeilen: 10-20

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.

**Quelle:** Hamill 2006
Seite(n): 278, Zeilen: 7-14

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.

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

### Verschleierung

**Untersuchte Arbeit:**
Seite: 240, Zeilen: 24-26

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 the data-sparse environment initially confronted by law enforcement and intelligence agencies.

**Quelle:** Hamill 2006
Seite(n): 278, Zeilen: 20-23

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.

**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

[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.

**Quelle:** Hamill 2006
Seite(n): 278, Zeilen: 21-23

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

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.

**Quelle:** Stephenson and Zelen 1989
Seite(n): 3, Zeilen: 28-33

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

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.

**Quelle:** Saxena et al. 2004
Seite(n): 94, Zeilen: 11-15

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
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.

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.

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)).
... the following roles in terrorist networks as proposed by Williams (2001):

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.

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.**

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.

4) **Guardians** guarantee network security and take essential measures to diminish 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).
Verschleierung

Untersuchte Arbeit: Seite: 247, Zeilen: 1-21

[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.]

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.

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 plasticity that is essential to avoid 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.

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

Verschleierung

Quelle: Lemieux_2003
Seite(n): 13, Zeilen: 7ff

[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 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 corruption and bribery to involuntary recruitment through pressure, occasionally supported by incentives and rewards.

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

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. 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.

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

Anmerkungen

continued from previous page

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.]

Anmerkungen

Even the final summary is copied from somewhere else.

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.

Anmerkungen

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

Sources (Quellen)
## [5.] Quelle:Nm/Berry et al. 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**  
**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**  
**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
## Quelle: Nm/Combatting 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**

**URL**
http://iis-db.stanford.edu/pubs/21057/Harmony_and_Disharmony-CTC.pdf

**Literaturverz.**
no

**Fußnoten**
no

---

## Quelle: Nm/DCSINT 2005

**Titel**

**Herausgeber**
US Army Training and Doctrine Command

**Ort**
Fort Leavenworth, Kansas

**Ausgabe**
Version 3.0

**Datum**
15. August 2005

**URL**

**Literaturverz.**
no

**Fußnoten**
yes

---

## 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**

**Literaturverz.**
yes

**Fußnoten**
yes

---

## 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
<table>
<thead>
<tr>
<th>Quelle:</th>
<th>Nm/Lemieux 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autor</td>
<td>Vincent Lemieux</td>
</tr>
<tr>
<td>Titel</td>
<td>Criminal Networks</td>
</tr>
<tr>
<td>Ort</td>
<td>Ottawa</td>
</tr>
<tr>
<td>Jahr</td>
<td>2003</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quelle:</th>
<th>Nm/Malin etal 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autor</td>
<td>Bradley Malin, Edoardo Airoldi, Kathleen M. Carley</td>
</tr>
<tr>
<td>Titel</td>
<td>A Network Analysis Model for Disambiguation of Names in Lists</td>
</tr>
<tr>
<td>Zeitschrift</td>
<td>COMPUTATIONAL &amp; MATHEMATICAL ORGANIZATION THEORY</td>
</tr>
<tr>
<td>Verlag</td>
<td>Springer</td>
</tr>
<tr>
<td>Ausgabe</td>
<td>11</td>
</tr>
<tr>
<td>Datum</td>
<td>July 2005</td>
</tr>
<tr>
<td>Nummer</td>
<td>2</td>
</tr>
<tr>
<td>Seiten</td>
<td>119-139</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quelle:</th>
<th>Nm/Padhy 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autor</td>
<td>Prafullah Padhy</td>
</tr>
<tr>
<td>Titel</td>
<td>Organised Crime</td>
</tr>
<tr>
<td>Ort</td>
<td>Delhi (India)</td>
</tr>
<tr>
<td>Verlag</td>
<td>Isha Books</td>
</tr>
<tr>
<td>Jahr</td>
<td>2006</td>
</tr>
<tr>
<td>Anmerkung</td>
<td>Chapter 7 &quot;Organised Crime and Terrorism&quot; is nothing else but an americanized copy of Shelley (2002).</td>
</tr>
<tr>
<td>ISBN</td>
<td>81-8205-348-X</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quelle:</th>
<th>Nm/Penzar etal 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autor</td>
<td>Dražen Penzar, Armano Srbjinićević</td>
</tr>
<tr>
<td>Titel</td>
<td>About Modelling of complex networks with applications to terrorist group modelling</td>
</tr>
<tr>
<td>Zeitschrift</td>
<td>Interdisciplinary Description of Complex Systems</td>
</tr>
<tr>
<td>Jahr</td>
<td>2005</td>
</tr>
<tr>
<td>Jahrhgang</td>
<td>3</td>
</tr>
<tr>
<td>Nummer</td>
<td>1</td>
</tr>
<tr>
<td>Seiten</td>
<td>27-43</td>
</tr>
<tr>
<td>ISSN</td>
<td>1334-4676</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>
### Reference 1

**Author**: Adam Perer, Ben Shneiderman  
**Title**: Balancing Systematic and Flexible Exploration 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 the paper contains 8 pages.  
**ISSN**: 1077-2626  

### Reference 2

**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  

### Reference 3

**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/
[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  

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)  

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.  

Literaturverz. no  
Fußnoten yes
<table>
<thead>
<tr>
<th>Quelle</th>
<th>Datum</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Dark Web Project</td>
<td>2010</td>
<td><a href="http://ai.eller.arizona.edu/research/terror/">http://ai.eller.arizona.edu/research/terror/</a></td>
</tr>
</tbody>
</table>
[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

Literaturverz.: no
Fußnoten: no

[53.] Quelle:Nm/Wikipedia-Bojinka-plot 2006

Titel: Bojinka plot

Literaturverz.: no
Fußnoten: no

[54.] Quelle:Nm/Wikipedia - Adnan Gulshair el Shukrijumah - 2006

Titel: Adnan Gulshair el Shukrijumah
Datum: June 2006

Literaturverz.: no
Fußnoten: yes


Titel: World Trade Center bombing (1993)
Datum: September 2006

Literaturverz.: no
Fußnoten: yes

[56.] Quelle:Nm/Wikipedia Riyadh compound bombings 2007

Titel: Riyadh compound bombings
Datum: 11. February 2007

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/

[58.] Quelle: Nm/Xu and Chen 2003

Autor: Jennifer Xu, Hsinchun Chen
Titel: Untangling Criminal Networks: A Case Study
Herausgeber: Chen, H et al.
Ort: Berlin, Heidelberg
Verlag: Springer-Verlag
Jahr: 2003
Nummer: 2665
Seiten: 232-248
DOI: 10.1007/3-540-44853-5_18
URL: http://www.springerlink.com/content/4rn8l185w0rvl931/

[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.: nein
Fußnoten: nein

Literaturverz.: nein
Fußnoten: nein

Literaturverz.: nein
Fußnoten: nein

Literaturverz.: nein
Fußnoten: nein
<table>
<thead>
<tr>
<th>Autor</th>
<th>Jennifer J. Xu, Hsinchun Chen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Titel</td>
<td>CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery</td>
</tr>
<tr>
<td>Zeitschrift</td>
<td>ACM Transactions on Information Systems</td>
</tr>
<tr>
<td>Datum</td>
<td>April 2005</td>
</tr>
<tr>
<td>Nummer</td>
<td>23 (2)</td>
</tr>
<tr>
<td>Seiten</td>
<td>201–226</td>
</tr>
<tr>
<td>Anmerkung</td>
<td>to be found as a reference in Nm, but with a wrong year</td>
</tr>
<tr>
<td>DOI</td>
<td>10.1145/1059981.1059984</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>yes</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Autor</th>
<th>Jennifer Xu, Byron Marshall, Siddharth Kaza, Hsinchun Chen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Titel</td>
<td>Analyzing and Visualizing Criminal Network Dynamics: A Case Study</td>
</tr>
<tr>
<td>Jahr</td>
<td>2004</td>
</tr>
<tr>
<td>Anmerkung</td>
<td>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 (<a href="http://books.google.de/books?id=zfvi37gYsGgC&amp;pg=PA360&amp;dq=A&amp;terrorist+network+is+primarily+a+social+network+in+which+individuals+connect+with+one+another+through&amp;source=bl&amp;ots=L9QluRgzaA&amp;sig=fOSN9Hkfw6hCmrAcdTlqve_6w&amp;hl=de&amp;sa=X&amp;ei=QC-GT4HwGYeR0AWPqbXMBw&amp;ved=0CCgQ6AEwAA#v=onepage&amp;q=Dynamic%20criminal%20network%20analysis%20is%20important%20for%20national%20security&amp;f=false">http://books.google.de/books?id=zfvi37gYsGgC&amp;pg=PA360&amp;dq=A&amp;terrorist+network+is+primarily+a+social+network+in+which+individuals+connect+with+one+another+through&amp;source=bl&amp;ots=L9QluRgzaA&amp;sig=fOSN9Hkfw6hCmrAcdTlqve_6w&amp;hl=de&amp;sa=X&amp;ei=QC-GT4HwGYeR0AWPqbXMBw&amp;ved=0CCgQ6AEwAA#v=onepage&amp;q=Dynamic%20criminal%20network%20analysis%20is%20important%20for%20national%20security&amp;f=false</a>), the page numbers given here refer to the version that is available online.</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Autor</th>
<th>Huijie Yang, Wenxu Wang, Tao Zhou, Binhong Wang, Fangcui Zhao</th>
</tr>
</thead>
<tbody>
<tr>
<td>Titel</td>
<td>Reconstruct the Hierarchical Structure in a Complex Network</td>
</tr>
<tr>
<td>Zeitschrift</td>
<td>arxiv.org</td>
</tr>
<tr>
<td>Datum</td>
<td>3. August 2005</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://arxiv.org/abs/physics/0508026v1">http://arxiv.org/abs/physics/0508026v1</a></td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Autor</th>
<th>Bin Zhao, Prithviraj Sen, Lise Getoor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Titel</td>
<td>Entity and Relationship Labeling in Affiliation Networks</td>
</tr>
<tr>
<td>Ort</td>
<td>Pittsburgh</td>
</tr>
<tr>
<td>Jahr</td>
<td>2006</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://www.mindswap.org/papers/2006/RelClzPIT.pdf">http://www.mindswap.org/papers/2006/RelClzPIT.pdf</a></td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
<tr>
<td>Titel</td>
<td>terrorism research</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Jahr</td>
<td>2005</td>
</tr>
<tr>
<td>Anmerkung</td>
<td>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</td>
</tr>
<tr>
<td>Literaturverz.</td>
<td>no</td>
</tr>
<tr>
<td>Fußnoten</td>
<td>no</td>
</tr>
</tbody>
</table>