Nm5/Report

Aus VroniPlag Wiki

This report is based on the findings of an ongoing plagiarism analysis (date: 05-02-2014). It is therefore no conclusive report and it is recommended to visit the page http://de.vroniplag.wikia.com/wiki/Nm5 for newer findings and further information.

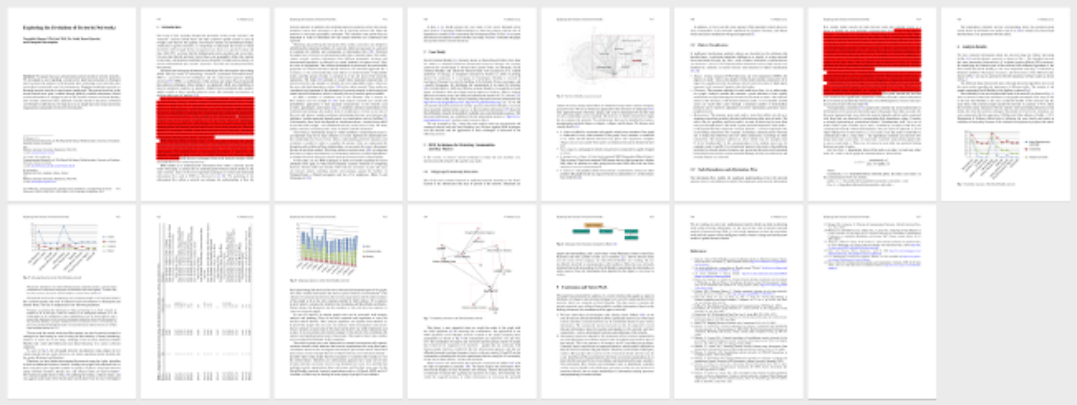
A critical discussion of the publication by Nasrullah Memon, Uffe Kock Wiil, Pir Abdul Rasool Qureshi and Panagiotis Karampelas: *Exploring the Evolution of Terrorist Networks*

in U.K. Wiil (ed.), Counterterrorism and Open Source Intelligence, Lecture Notes in Social Networks 2, 413-427, Springer-Verlag/Wien 2011 →ISBN 978-3-7091-0387-6 →Download (http://www.springerlink.com/content/r970122m77980211/)

Overview

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

- red="Verschleierung": the source of the text parallel is not given, the copied text will be somewhat modified.



Prominent findings of plagiarism

- Fragment 419 02: About half a page is taken from an unnamed source with only minor adjustments apart from the substitution of "terrorists" for "academic colleagues" and correspondingly "foot-soldier" for "assistant professor" and "cell leader" for "department chairperson".

Statistics

- Currently there are 4 reviewed fragments documented, that are considered to be plagiarism. For 4 of them there is no reference given to the source used („Verschleierungen“ and „Komplettplagiate“). For 0 fragments the source is given, but the extent of the used text is not made clear („Bauernopfer“).

- The publication has 14 pages that have been analyzed. On a total of 2 of these pages plagiarism has been documented. This represents a percentage of **14.3%**. The 14 analyzed pages break down with respect to the amount of plagiarism encountered as follows:

Percentage plagiarism	Number of pages
No plagiarism documented	12
0%-50% Plagiarism	2
50%-75% Plagiarism	0
75%-100% Plagiarism	0

  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 6%** of the main part of the publication.

- In all, text was taken from 4 sources.

Duplication

The paper is to a large degree identical to the publication Wiil et al. (2010b) (retracted) by three of the authors of the paper. In comparison to this earlier publication, only the introduction has been extended, a short section at the end of chapter 4 and the section 3.3 have been added. The rest of the publication is a verbatim copy of the previous paper with only very minor adjustments. More than 75% of the text is identical to text in the 2010 article and so are 5 of 6 figures and one table.

In addition, much of the section 3.3 can already be found in Memon et al.(2007b).

The following chart illustrates the amount of duplicated text. The colours show two sources of duplicated text:

- blue: Wiil et al. (2010b) (retracted)
- green: Memon et al.(2007b)

References

Memon, Hicks, Larsen (2007b) (http://www.springerlink.com/content/p6w523g8481n2427/) : *How Investigative Data Mining Can Help Intelligence Agencies to Discover Dependence of Nodes in Terrorist Networks* in: R. Alhajj et al. (Eds.): ADMA 2007, LNAI 4632, pp. 430–441, 2007. Springer Berlin Heidelberg

Wiil, Memon, Karampelas (2010b) (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5563064&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5563064) : *Detecting New Trends in Terrorist Networks* in: 2010 International Conference on Advances in Social Networks Analysis and Mining, 435-440, 978-0-7695-4138-9/10 IEEE, DOI 10.1109/ASONAM.2010.73 (retracted)

Appendix 1: Fragments

Remark on the colouring

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

Remark on the line numbering

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

4 gesichtete, geschützte Fragmente

[1.] Nm5/Fragment 414 20

Verschleierung

Untersuchte Arbeit: Seite: 414, Zeilen: 20-25	**Quelle: Han_Kamber_2006 Seite(n): 560, 561, Zeilen: 560: last lines; 561: 1ff** Farbig
How can we mine terrorist networks? Traditional methods of machine learning and data mining, taking a random sample of homogeneous objects from a single relation as input, may not be appropriate. The data comprising terrorist networks tend to be heterogeneous, multi-relational, and semi-structured. IDM embodies descriptive and predictive modeling. By considering links (relationships between the entities), more information is made available to the mining process.	*"How can we mine social networks?"* Traditional methods of machine learning and data mining, taking, as input, a random sample of homogenous [sic] objects from a single [page 561] relation, may not be appropriate here. The data comprising social networks tend to be heterogeneous, multirelational, and semi-structured.[...] It embodies descriptive and predictive modeling. By considering links (the relationships between objects), more information is made available to the mining process.

Anmerkungen

The source is not mentioned anywhere in the paper.

Also the formatting with italics is parallel.

[2.] Nm5/Fragment 414 25

Verschleierung

Untersuchte Arbeit: **Seite: 414, Zeilen: 25-31**	**Quelle: Svenson et al 2006** **Seite(n): 3, Zeilen: 1ff**
Mathematical methods used in the research on IDM [12–15] are clearly relevant to intelligence analysis and may provide tools and techniques to discover terrorist networks in their planning phase and thereby prevent terrorist acts from being carried out. Relevant patterns to investigate include connections between actors (meetings, messages), activities of the involved actors (specialized training, purchasing of equipment), and information gathering (time tables, visiting sites).	Social network analysis methods are clearly relevant to law enforcement intelligence work and may provide tools to discover criminal networks in their planning phase and thereby prevent terrorist acts and other large-scale crimes from being carried out. Relevant patterns to investigate include connections between actors (meetings, messages), activities of the involved actors (specialized training, purchasing of equipment) and information gathering (time tables, visiting sites).

Farbig

12. Memon, N., Larsen H.L.: Practical approaches for analysis, visualization and destabilizing terrorist networks. In: The proceedings of ARES 2006: The First International Conference on Availability, Reliability and Security, Vienna, Austria, IEEE Computer Society, pp. 906–913 (2006)

13. Memon, N., Larsen, H.L.: Practical algorithms of destabilizing terrorist networks. In the proceedings of IEEE Intelligence Security Conference, San Diego, Lecture Notes in Computer Science, Vol. 3976: pp. 398–411. Springer, Berlin (2006)

14. Memon, N., Larsen, H.L.: Detecting Terrorist Activity Patterns using Investigative Data Mining Tool. International Journal of Knowledge and System Sciences, 3(1), 43–52 (2006)

15. Memon, N., Qureshi, A.R.: Destabilizing terrorist networks. In WSEAS Transactions on Computers. **11**(4), 1649–1656 (2005)

Anmerkungen

The source is not mentioned anywhere in the paper.

[3.] Nm5/Fragment 414 32

Verschleierung

Untersuchte Arbeit: **Seite: 414, Zeilen: 32-37**	**Quelle: Koschade 2005** **Seite(n): 2, 3, Zeilen: 2: 6-8; 3: 31ff**
IDM offers the ability to firstly map a covert cell, and to measure the specific structural and interactional criteria of such a cell. IDM aims to connect the dots between individuals and map and measure complex, covert, human groups, and organizations. The methods focus on uncovering the patterns of interaction, and correctly interpreting these networks to predict behaviors 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. [page 3] This framework aims to connect the dots between individuals and "map and measure complex, sometimes covert, human groups and organisations".[8] The method focuses on uncovering the patterning of people's interaction,[9] and correctly interpreting these networks assists "in predicting behaviour and decision-making within the network".[10]

Farbig

8 Krebs, V. (2002) "Mapping Networks of Terrorist Cells", *Connections*, Vol. 24, 3, pp. 43-52.

9 Freeman, L. (nd) 'The Study of Social Networks', *The International Network for Social Network Analysis*, Retrieved May 17, 2004, from http://www.sfu.ca/~insna/INSNA/na_inf.html.

10 Renfro, R. & Deckro, R. (2001). "A Social Network Analysis of the Iranian Government", paper presented at *69th MORS Symposium*, 12-14 June, 2001, p. 4.

Anmerkungen

The source is not mentioned anywhere in the paper.

[4.] Nm5/Fragment 419 02

Verschleierung

Untersuchte Arbeit: Seite: 419, Zeilen: 2-20	Quelle: Katz et al 2004 Seite(n): 308, 309, Zeilen: 308: 23ff; 309: 1ff
In the social network literature, researchers have examined a broad range of types of ties [19]. 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 bomb making material or other resources to whom), and proximity ties (who is spatially or electronically close to whom). Networks are typically multiplex, that is, actors share more than one type of tie. For example, two terrorists might have a formal tie (one is a foot-soldier or a newly recruited person in the terrorist cell and reports to the other, who is the cell leader) and an affective tie (they are friends); and may also have a proximity tie (they are residing in the same apartment and their flats are two doors away on the same floor).	Network researchers have examined a broad range of types of ties. These include communication ties (such as who talks to whom, or who gives information or advice to whom), formal ties (such as who reports to whom), affective ties (such as who likes whom, or who trusts whom), material or work flow ties (such as who gives money or other resources to whom), proximity ties (who is spatially or electronically close to whom), and cognitive ties (such as who knows who knows whom). Networks are typically mutiplex [sic], that is, actors share more than one type of tie. For example, two academic colleagues might have a formal tie (one is an assistant professor and reports to the other, who is the department chairperson)
Network researchers have distinguished between strong ties (such as family and friends) and weak ties such as acquaintances [9, 10]. This distinction will involve a multitude of facets, including affect, mutual obligations, reciprocity, and intensity.	[page 309]
In information flow, the 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.	and an affective tie (they are friends) and a proximity tie (their offices are two doors away).
	Network researchers have distinguished between strong ties (such as family and friends) and weak ties (such as acquaintances) (Granovetter, 1973, 1982). This distinction can involve a multitude of facets, including affect, mutual obligations, reciprocity, and intensity. Strong ties are particularly valuable when an individual seeks socioemotional support and often entail a high level of trust. Weak ties are more valuable when individuals are seeking diverse or unique information from someone outside their regular frequent contacts.
9. Granovetter, M.: The Strength of Weak Ties. Am. J. Sociol. **81**, 1287–1303 (1973)	Granovetter,M. (1973). The strength of weak ties. *American Journal of Sociology*, *81*, 1287-1303.
10. Granovetter, M.: The Strength of Weak Ties: A Network Theory Revisited. In: Collins, R.(ed.) Sociological Theory, pp. 105–130 (1982)	Granovetter,M. (1982). The strength of weak ties: A network theory revisited. In R. Collins (Ed.), *Sociological theory 1983* (pp. 105-130). San Francisco: Jossey-Bass.
19. Monge, P.R., Contractor, N.: Theories of Communication Networks. Oxford University Press, New York (2003)	

Farbig

Anmerkungen

The source is not mentioned anywhere in the paper.

The authors of the paper substitute here "terrorists" for "academic colleagues" and correspondingly "foot-soldier" for "assistant professor" and "cell leader" for "department chairperson".

Appendix 2: Sources

[1.] Quelle:Nm5/Han Kamber 2006

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

[2.] Quelle:Nm5/Katz et al 2004

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

[3.] Quelle:Nm5/Koschade 2005

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

[4.] Quelle:Nm5/Svenson et al 2006

Autor	Pontus Svenson, Per Svensson, Hugo Tullberg
Titel	Social Network Analysis And Information Fusion For AntiTerrorism
Zeitschrift	Proc. CIMI
Jahr	2006
URL	http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.7470 http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=783D9DC8CE7E0EAA204AF94B579E0FA6?doi=10.1.1.64.7470&rep=rep1&type=pdf
Webcite	http://www.webcitation.org/6N64iPq0E
Literaturverz.	no
Fußnoten	no

Eine Diskussion beginnen