CONNECTIONS 24(3): 43-52

Mapping Networks of Terrorist Cells

Valdis E. Krebs
orgnet.com

This paper looks at the difficulty in mapping covert networks. Analyzing networks after an event is fairly easy for prosecution purposes. Mapping covert networks to prevent criminal activity is much more difficult. We examine the network surrounding the tragic events of September 11th, 2001. Through public data we are able to map a portion of the network centered around the 19 dead hijackers. This map gives us some insight into the terrorist organization, yet it is incomplete. Suggestions for further work and research are offered.

INTRODUCTION AND BACKGROUND

We were all shocked by the tragic events of September 11, 2001. In the non-stop stream of news and analysis one phrase was constantly repeated and used in many contexts – "terrorist network." Everyone talked about this concept, and described it as amorphous, invisible, resilient, dispersed and other terms that made it difficult to visualize what this structure really looks like. I set out to map this network of terrorist cells that had so affected all of our lives.

I would be mapping a 'project team' – much like the legal, overt groups I had mapped in countless consulting assignments. Both overt and covert project teams have tasks to complete, information to share, funding to obtain and administer, schedules to meet, work to coordinate, and objectives to accomplish. How a normal project team does all of that is easy to map and measure using several set of ties – task, resource, strategy and expertise links. I was surprised at the difficulty of this particular effort – both in data definition and discovery.

My data sources were publicly released information reported in major newspapers such as the New York Times, the Wall Street Journal, the Washington Post, and the Los Angeles Times. As I monitored the investigation, it was apparent that the investigators would not be releasing all

pertinent network/relationship information and actually may be releasing misinformation to fool the enemy. I soon realized that the data was not going to be as complete and accurate as I had grown accustomed to in mapping and measuring organizational networks.

For guidance I turned to previous work by social network theorists who had studied covert, secret, or illegal networks. I found three excellent papers that formed a working foundation for the knowledge I would use to pursue this project. Malcolm Sparrow (Sparrow 1991) has an excellent overview of the application of social network analysis to criminal activity. Sparrow describes three problems of criminal network analysis that I soon encountered.

1. Incompleteness – the inevitability of missing nodes and links that the investigators will not uncover.
2. Fuzzy boundaries – the difficulty in deciding who to include and who not to include.
3. Dynamic – these networks are not static, they are always changing. Instead of looking at the presence or absence of a tie between two individuals, Sparrow suggests looking at the waxing and waning strength of a tie depending upon the time and the task at hand.

Wayne Baker and Robert Faulkner (Baker and Faulkner 1993) suggest looking at archival data to derive relationship data. The data they used to analyze illegal price-fixing networks were mostly court documents and sworn testimony. This data included accounts of observed interpersonal relationships from various witnesses. The hijackers of September 11th were not directly observed by others in great detail.

Bonnie Erickson (Erickson 1981) reveals the importance of trusted prior contacts for the effective functioning of a secret society. The 19 hijackers appeared to have come from a network that had formed while they were completing terrorist training in Afghanistan. Many were school chums from many years ago, some had lived together for years, and others were related by kinship ties. Deep trusted ties, that were not easily visible to outsiders, wove this terror network together.

Data Gathering

Within one week of the attack, information from the investigation started to become public. We soon knew there were 19 hijackers, which planes they were on, and which nation's passports they had used to get into the country. As more information about the hijackers' past was uncovered I decided to map links of three strengths (and corresponding thicknesses). The tie strength would largely be governed by the amount of time together by a pair of terrorists. Those living together or attending the same school or the same classes/training would have the strongest ties. Those travelling together and participating in meetings together would have ties of moderate strength and medium thickness. Finally, those who were recorded as having a financial transaction together, or an occasional meeting, and no other ties, I sorted into the dormant tie category – they would rarely interact. These relationships were shown with the thinnest links in the network.

I started my mapping project upon seeing the matrix in Figure1 on the web site of the Sydney Morning Herald (AU) (Sydney Morning Herald, 2001). This was the first attempt I had seen to visually organize the data that was gradually becoming available two weeks after the tragedy.

Soon after the matrix in Figure 1 was published, the Washington Post released a more detailed matrix of how the hijackers had spent their time in the USA and with whom (Washington Post, 2001). The most detailed document of the hijackers relationships and activity was released in December 2001 in the Indictment of Zacarias Moussaoui (Department of Justice, 2001).

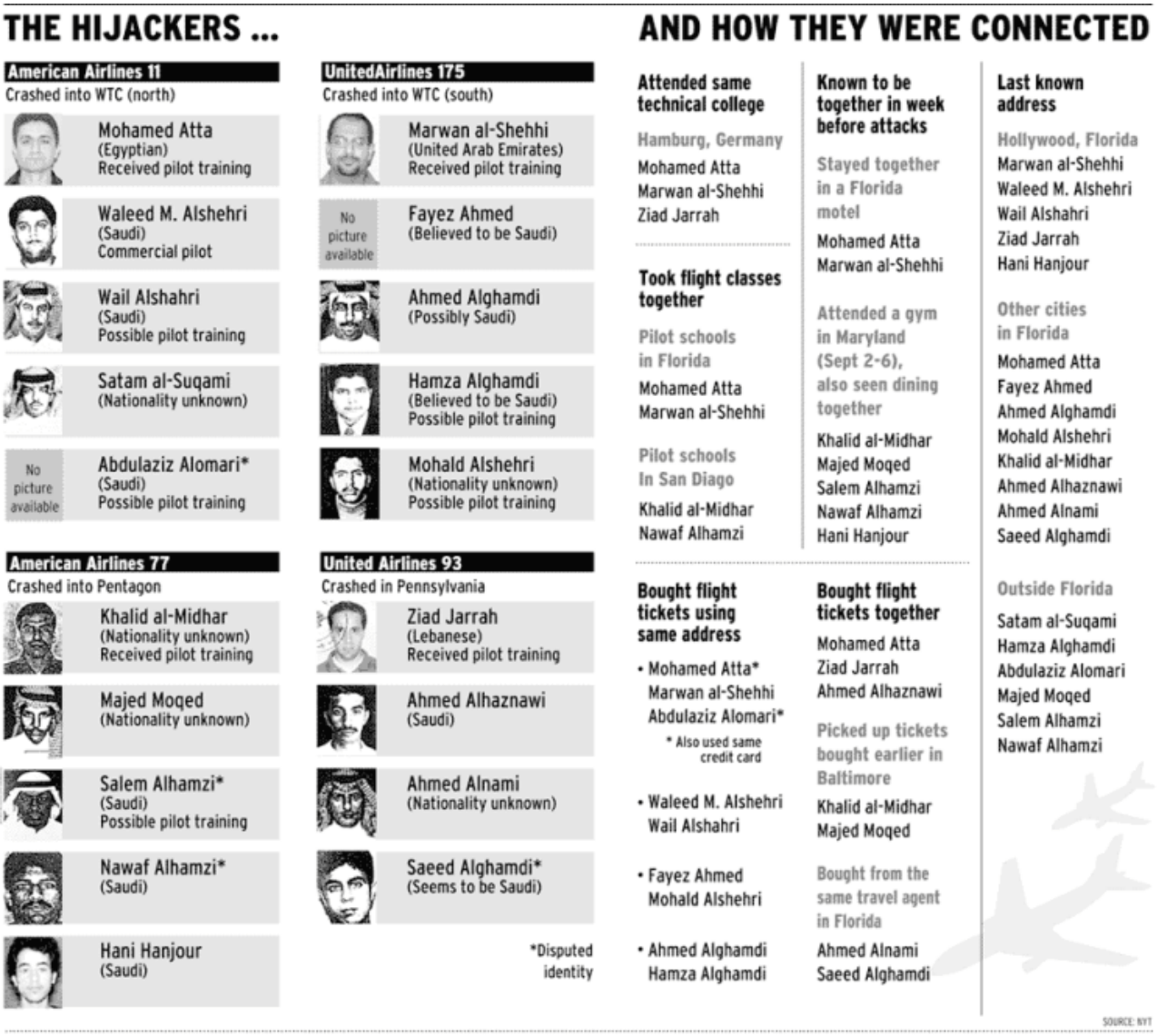


Figure 1. Early Hijacker Matrix

Once the names of the 19 hijackers were public, discovery about their background and ties seemed to accelerate. From two to six weeks after the event, it appeared that a new relationship or node was added to the network on a daily basis. In addition to tracking the newspapers mentioned, I started to search for the terrorists' names using the Google search engine [1]. Although I would find information about each of the 19 hijackers, rarely would I find information from the search engine that was not reported by the major newspapers I was tracking. Finding information that was not duplicated in one of the prominent newspapers made me suspicious. Several false stories appeared about a cell in Detroit. These stories, originally reported with great fanfare, were proven false within one week. This made me even more cautious about which sources I used to add a link or a node to the network.

By the middle of October enough data was available to start seeing patterns in the hijacker network. Initially, I examined the prior trusted contacts (Erickson, 1981) – those ties formed through living and learning together. The network appeared in the shape of a serpent (Figure 2) – how appropriate, I thought.

[1] http://www.google.com

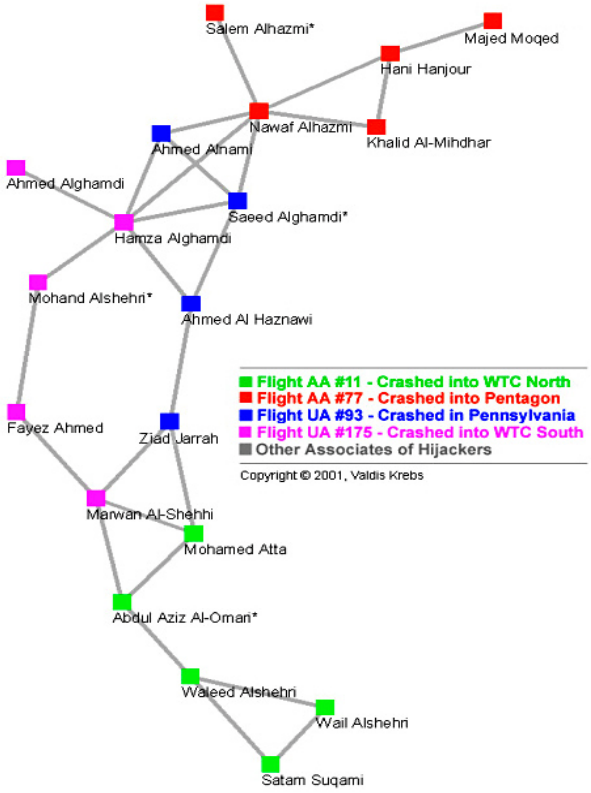


Figure 2 Trusted Prior Contacts

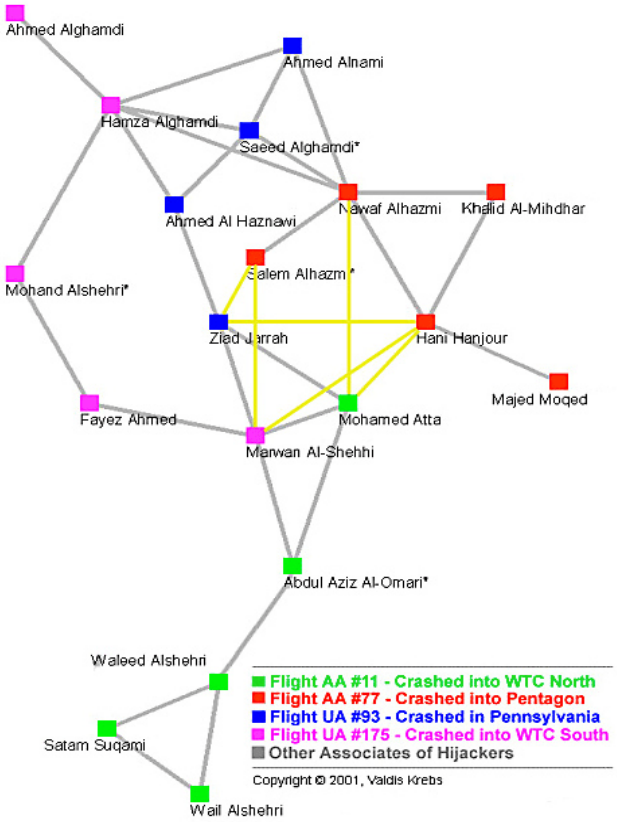


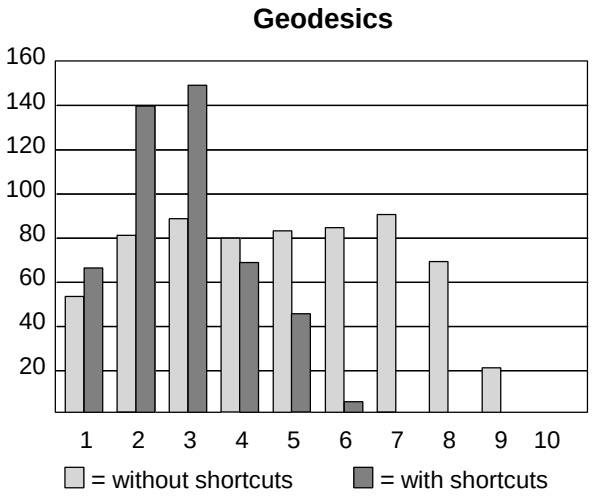
Figure 3 Trusted Prior Contacts + Meeting Ties [shortcuts]

I was amazed at how sparse the network was and how distant many of the hijackers on the same team were from each other. Many pairs of team members where beyond the horizon of observability (Friedkin, 1983) from each other – many on the same flight were more than 2 steps away from each other. Keeping cell members distant from each other, and from other cells, minimizes damage to the network if a cell member is captured or otherwise compromised. Usama bin Laden even described this strategy on his infamous video tape which was found in a hastily deserted house in Afghanistan. In the transcript (Department of Defense, 2001) bin Laden mentions:

Those who were trained to fly didn't know the others. One group of people did not know the other group.

The metrics for the network in Figure 2 are shown below and in Table 1. We see a very long mean path length, 4.75, for a network of less than 20 nodes. From this metric and bin Laden's comments above we see that covert networks trade efficiency for secrecy.

	no shortcuts	with shortcuts
Group Size	19	19
Potential Ties	342	342
Actual Ties	54	66
Density	16 %	19%



Yet, work has to be done, plans have to be executed. How does a covert network accomplish its goals? Through the judicious use of transitory short-cuts (Watts, 1999) in the network. Meetings are held that connect distant parts of the network to coordinate tasks and report progress. After the coordination is

accomplished, the cross-ties go dormant until the need for their activity arises again. One well-documented meeting of the hijacker network took place in Las Vegas. The ties from this and other documented meetings are shown in gold in Figure 3.

Table 1. Without shortcuts

Name	Clustering Coefficient	Mean Path Length	Shortcuts
Satam Suqami	1.00	5.22	0.00
Wail Alshehri	1.00	5.22	0.00
Majed Moqed	0.00	4.67	0.00
Waleed Alshehri	0.33	4.33	0.33
Salem Alhazmi*	0.00	3.89	0.00
Khalid Al-Mihdhar	1.00	3.78	0.00
Hani Hanjour	0.33	3.72	0.00
Abdul Aziz Al-Omari*	0.33	3.61	0.33
Ahmed Alghamdi	0.00	3.50	0.00
Ahmed Alnami	1.00	3.17	0.00
Mohamed Atta	0.67	3.17	0.00
Marwan Al-Shehhi	0.33	3.06	0.25
Fayez Ahmed	0.00	2.94	1.00
Nawaf Alhazmi	0.27	2.94	0.00
Ziad Jarrah	0.33	2.83	0.33
Mohand Alshehri*	0.00	2.78	1.00
Saeed Alghamdi*	0.67	2.72	0.00
Ahmed Al Haznawi	0.33	2.67	0.33
Hamza Alghamdi	0.27	2.56	0.17
Overall	**0.41**	**4.75**	**0.19**

Table 2. With shortcuts

Name	Clustering Coefficient	Mean Path Length	Shortcuts
Satam Suqami	1.00	3.94	0.00
Wail Alshehri	1.00	3.94	0.00
Ahmed Alghamdi	0.00	3.22	0.00
Waleed Alshehri	0.33	3.06	0.33
Majed Moqed	0.00	3.00	0.00
Mohand Alshehri*	0.00	2.78	1.00
Khalid Al-Mihdhar	1.00	2.61	0.00
Ahmed Alnami	1.00	2.56	0.00
Fayez Ahmed	0.00	2.56	1.00
Ahmed Al Haznawi	0.33	2.50	0.33
Saeed Alghamdi*	0.67	2.44	0.00
AbdulAziz Al-Omari*	0.33	2.33	0.33
Hamza Alghamdi	0.27	2.28	0.17
Salem Alhazmi*	0.33	2.28	0.33
Ziad Jarrah	0.40	2.17	0.20
Marwan Al-Shehhi	0.33	2.06	0.17
Hani Hanjour	0.33	2.06	0.00
Mohamed Atta	0.50	1.94	0.00
Nawaf Alhazmi	0.24	1.94	0.14
Overall	**0.42**	**2.79**	**0.18**

* suspected to have false identification

Six (6) shortcuts were added to the network temporarily in order to collaborate and coordinate. These shortcuts dropped the mean path length in the network by over 40% thus improving the information flow in the network. There is a constant struggle between keeping the network hidden and actively using it to accomplish objectives (Baker and Faulkner, 1993).

The 19 hijackers did not work alone. They had accomplices who did not get on the planes. These co-conspirators were conduits for money and also provided needed skills and knowledge. Figure 4 shows the hijackers and their immediate network neighbourhood – their identified direct contacts.

After one month of investigation it was 'common knowledge' that Mohamed Atta was the ring leader of this conspiracy. Again, bin Laden verified this in the video tape (Department of Defense, 2001). Looking at the diagram he has the most connections. In Table 3 we see that Atta scores the highest on Degrees, and Closeness but not Betweenness centrality (Freeman 1979). These metrics do not necessarily confirm his leader status. We are obviously missing nodes and ties in this network. Centrality measures are very sensitive to minor changes in nodes and links. A discovery of a new conspirator along with new ties, or the uncovering of a tie amongst existing nodes can alter who comes out on top in the Freeman centralities. Recent converts to social network analysis are thrilled about what these metrics may show (Stewart 2001), experienced players urge caution[2].

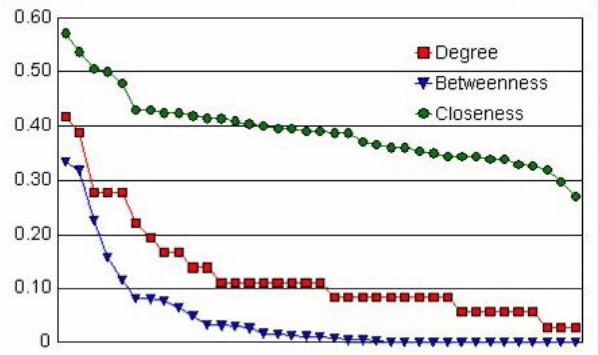
[2] Email correspondence with Ron Burt, Wayne Baker, Barry Wellman, Peter Klerks

Table 3. Hijackers' Network Neighborhood

Group Size	37
Potential Ties	1332
Actual Ties	170
Density	13%

Geodesics

length	#
1	170
2	626
3	982
4	558
5	136
6	0



Degrees		Betweenness		Closeness	
0.417	Mohamed Atta	0.334	Nawaf Alhazmi	0.571	Mohamed Atta
0.389	Marwan Al-Shehhi	0.318	Mohamed Atta	0.537	Nawaf Alhazmi
0.278	Hani Hanjour	0.227	Hani Hanjour	0.507	Hani Hanjour
0.278	Nawaf Alhazmi	0.158	Marwan Al-Shehhi	0.500	Marwan Al-Shehhi
0.278	Ziad Jarrah	0.116	Saeed Alghamdi*	0.480	Ziad Jarrah
0.222	Ramzi Bin al-Shibh	0.081	Hamza Alghamdi	0.429	Mustafa al-Hisawi
0.194	Said Bahaji	0.080	Waleed Alshehri	0.429	Salem Alhazmi*
0.167	Hamza Alghamdi	0.076	Ziad Jarrah	0.424	Lotfi Raissi
0.167	Saeed Alghamdi*	0.064	Mustafa al-Hisawi	0.424	Saeed Alghamdi*
0.139	Lotfi Raissi	0.049	Abdul Aziz Al-Omari*	0.419	Abdul Aziz Al-Omari*
0.139	Zakariya Essabar	0.033	Satam Suqami	0.414	Hamza Alghamdi
0.111	Agus Budiman	0.031	Fayez Ahmed	0.414	Ramzi Bin al-Shibh
0.111	Khalid Al-Mihdhar	0.030	Ahmed Al Haznawi	0.409	Said Bahaji
0.111	Mounir El Motassadeq	0.026	Nabil al-Marabh	0.404	Ahmed Al Haznawi
0.111	Mustafa al-Hisawi	0.016	Raed Hijazi	0.400	Zakariya Essabar
0.111	Nabil al-Marabh	0.015	Lotfi Raissi	0.396	Agus Budiman
0.111	Rayed Abdullah	0.012	Mohand Alshehri*	0.396	Khalid Al-Mihdhar
0.111	Satam Suqami	0.011	Khalid Al-Mihdhar	0.391	Ahmed Alnami
0.111	Waleed Alshehri	0.010	Ramzi Bin al-Shibh	0.391	Mounir El Motassadeq
0.083	Abdul Aziz Al-Omari*	0.007	Salem Alhazmi*	0.387	Fayez Ahmed
0.083	Abdussattar Shaikh	0.004	Ahmed Alghamdi	0.387	Mamoun Darkazanli
0.083	Ahmed Al Haznawi	0.004	Said Bahaji	0.371	Zacarias Moussaoui
0.083	Ahmed Alnami	0.002	Rayed Abdullah	0.367	Ahmed Khalil Al-Ani
0.083	Fayez Ahmed	0.000	Abdussattar Shaikh	0.360	Abdussattar Shaikh
0.083	Mamoun Darkazanli	0.000	Agus Budiman	0.360	Osama Awadallah
0.083	Osama Awadallah	0.000	Ahmed Alnami	0.353	Mohamed Abdi
0.083	Raed Hijazi	0.000	Ahmed Khalil Al-Ani	0.350	Rayed Abdullah
0.083	Salem Alhazmi*	0.000	Bandar Alhazmi	0.343	Bandar Alhazmi
0.056	Ahmed Alghamdi	0.000	Faisal Al Salmi	0.343	Faisal Al Salmi
0.056	Bandar Alhazmi	0.000	Majed Moqed	0.343	Mohand Alshehri*
0.056	Faisal Al Salmi	0.000	Mamoun Darkazanli	0.340	Majed Moqed
0.056	Mohand Alshehri*	0.000	Mohamed Abdi	0.340	Waleed Alshehri
0.056	Wail Alshehri	0.000	Mounir El Motassadeq	0.330	Nabil al-Marabh
0.056	Zacarias Moussaoui	0.000	Osama Awadallah	0.327	Raed Hijazi
0.028	Ahmed Khalil Al-Ani	0.000	Wail Alshehri	0.319	Ahmed Alghamdi
0.028	Majed Moqed	0.000	Zacarias Moussaoui	0.298	Satam Suqami
0.028	Mohamed Abdi	0.000	Zakariya Essabar	0.271	Wail Alshehri
0.128	MEAN	0.046	MEAN	0.393	MEAN
0.306	CENTRALIZATION	0.296	CENTRALIZATION	0.372	CENTRALIZATION

* suspected to have false identification

Prevention or Prosecution?

Currently, social network analysis is applied more to the prosecution, not the prevention, of criminal activities. SNA has a long history of application to evidence mapping in both fraud and criminal conspiracy cases. Once investigators have a suspect they can start to build an ego network by looking at various sources of relational information. These sources are many and provide a quickly focusing picture of illegal activity. These sources include (DIA, 2000):

- Credit files, bank accounts and the related transactions
- Telephone calling records
- Electronic mail, instant messaging, chat rooms, and web site visits
- Court records
- Business, payroll and tax records
- Real estate and rental records
- Vehicle sale and registration records

As was evident with the September 11th hijackers, once the investigators knew who to look at, they quickly found the connections amongst the hijackers and also discovered several of the hijackers' alters. We must be careful of 'guilt by association'. Being an alter of a terrorist does not prove guilt – but it does invite investigation.

The big question remains – why wasn't this attack predicted and prevented? Everyone expects the intelligence community to uncover these covert plots and stop them before they are executed. Occasionally plots are uncovered and criminal networks are disrupted. But this is very difficult to do. How do you discover a network that focuses on secrecy and stealth?

Covert networks often don't behave like normal social networks (Baker and Faulkner, 1993). Conspirators don't form many new ties outside of the network and often minimize the activation of existing ties inside the network. Strong ties, which were frequently formed years ago in school and training camps, keep the cells interconnected. Yet, unlike normal social networks, these strong ties remain mostly dormant and therefore hidden. They are only activated when absolutely necessary. Weak ties were almost non-existent between members of the hijacker network and outside contacts. It was often reported that the hijackers kept to themselves. They would rarely interact with outsiders, and then often one of them would speak for the whole group. A minimum of weak ties reduces the visibility into the network, and chance of leaks out of the network.

In a normal social network, strong ties reveal the cluster of network players – it is easy to see who is in the group and who is not. In a covert network, because of their low frequency of activation, strong ties may appear to be weak ties. The less active the network, the more difficult it is to discover. Yet, the covert network has a goal to accomplish. Network members must balance the need for secrecy and stealth with the need for frequent and intense task-based communication (Baker and Faulkner 1993). The covert network must be active at times. It is during these periods of activity that they may be most vulnerable to discovery.

The hijacker's network had a hidden strength – massive redundancy through trusted prior contacts. The ties forged in school, through kinship, and training/fighting in Afghanistan made this network very resilient. These ties were solidly in place as the hijackers made their way to America. While in America, these strong ties were rarely active – used only for planning and coordination. In effect these underlying strong ties were mostly invisible during their stay in America. It was only after the tragic event, that intelligence from Germany and other countries, revealed this dense under-layer of this violent network. The dense connections of the 'Hamburg cell' are obvious in Figure 4.

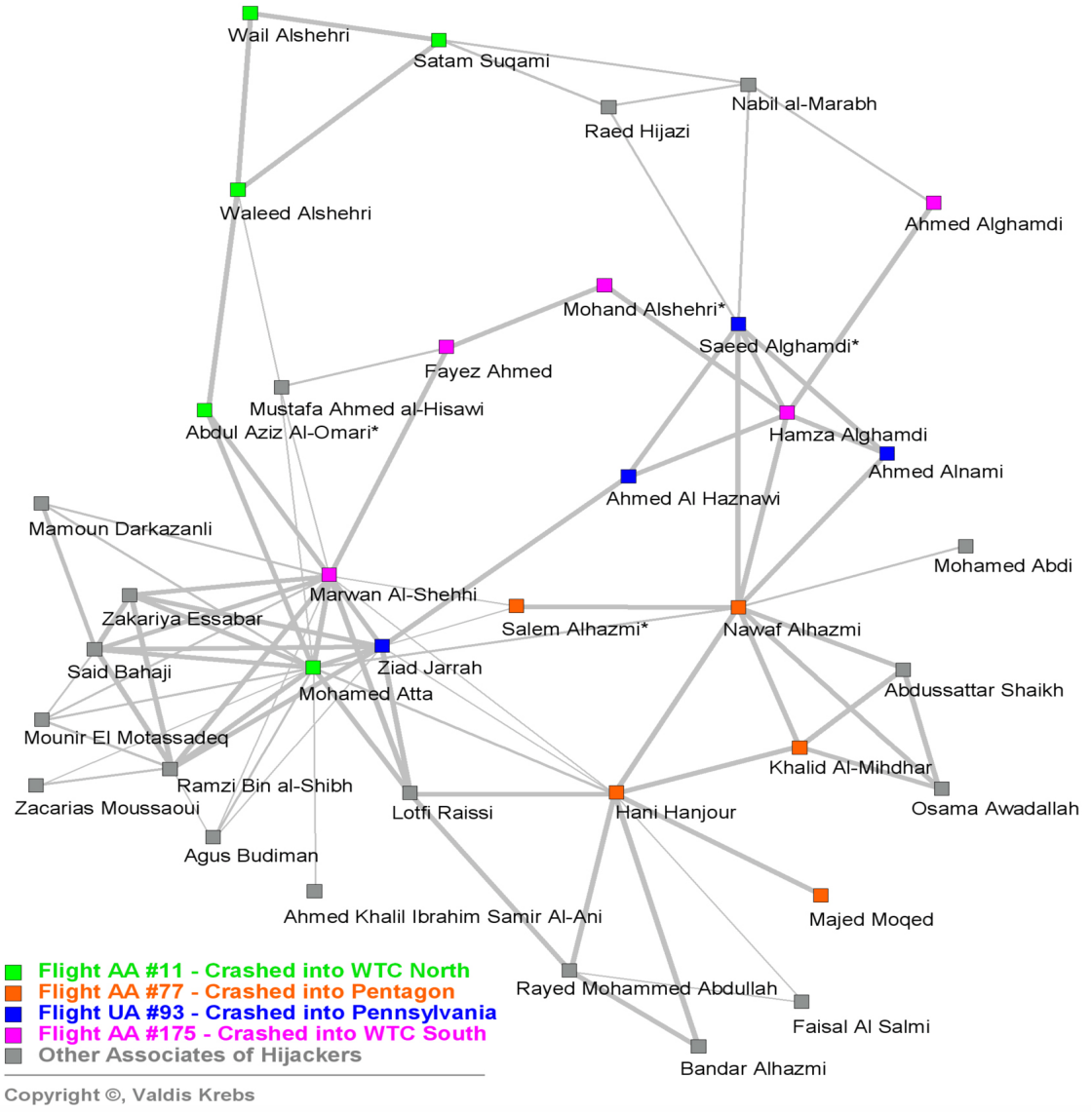


Figure 4. Hijacker's Network Neighborhood

This dense under-layer of prior trusted relationships made the hijacker network both stealth and resilient. Although we don't know all of the internal ties of the hijackers' network it appears that many of the ties were concentrated around the pilots. This is a risky move for a covert network. Concentrating both unique skills and connectivity in the same nodes makes the network easier to disrupt – once it is discovered. Peter Klerks (Klerks 2001) makes an excellent argument for targeting those nodes in the network that have unique skills. By removing those necessary skills from the project, we can inflict maximum damage to the project mission and goals. It is possible that those with unique skills would also have unique ties within the network. Because of their unique human capital and their high social capital the pilots were the richest targets for removal from the network. Unfortunately they were not discovered in time.

Conclusion

To draw an accurate picture of a covert network, we need to identify task and trust ties between the conspirators. The same four relationships we map in business organizations would tell us much about illegal organizations. This data is occasionally difficult to unearth with cooperating clients. With covert criminals, the task is enormous, and may be impossible to complete. Table 4 below lists multiple project networks and possible data sources about covert collaborators.

Table 4. Networks to Map

Relationship / Network	**Data Sources**
1. Trust	Prior contacts in family, neighborhood, school, military, club or organization. Public and court records. Data may only be available in suspect's native country.
2. Task	Logs and records of phone calls, electronic mail, chat rooms, instant messages, web site visits. Travel records. Human intelligence – observation of meetings and attendance at common events.
3. Money & Resources	Bank account and money transfer records. Pattern and location of credit card use. Prior court records. Human intelligence – observation of visits to alternate banking resources such as Hawala.
4. Strategy & Goals	Web sites. Videos and encrypted disks delivered by courier. Travel records. Human intelligence – observation of meetings and attendance at common events

Of course, the common network researcher will not have access to many of these sources. The researcher's best sources may be public court proceedings which contain much of this data (Baker and Faulkner, 1993), (Department of Justice, 2001).

The best solution for network disruption may be to discover possible suspects and then, via snowball sampling, map their ego networks – see whom else they lead to, and where they overlap. To find these suspects it appears that the best method is for diverse intelligence agencies to aggregate their information – their individual pieces to the puzzle – into a larger emergent map. By sharing information and knowledge, a more complete picture of possible danger can be drawn. In my data search I came across many news accounts where one agency, or country, had data that another would have found very useful. To win this fight against terrorism it appears that the good guys have to build a better information and knowledge sharing network than the bad guys (Ronfeldt and Arquilla, 2001).

REFERENCES

Baker, W.E. and R.R. Faulkner. 1993. The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review* 58(6) 837-860.

Defense Intelligence Agency. 2000. *Criminal Network Analysis Training Course*. http://www.oss. net/Papers/training/Lesson007Guide.html

Erickson, B.H. 1981. Secret societies and social structure. *Social Forces* 60(1): 188-210.

Freeman, L.C. 1979. Centrality in social networks: conceptual clarification. *Social Networks* 1: 215-239.

Friedkin, N.E. 1983. Horizons of observability and limits of informal control in organizations.*Social Forces* 62: 54-77.

Klerks, P. 2001. The network paradigm applied to criminal organizations", *Connections* 24(3) xx-yy.

Krebs, V.E. 2001. Network Metrics. InFlow 3.0 Users' Manual.

Ronfeldt, D. and J. Arquilla. 2001. Networks, netwars, and the fight for the future. *First Monday,* 6(10). http://www.firstmonday.dk/issues/issue6_10/index.html

Stewart, T. 2001. Six degrees of Mohamed Atta. *Business 2.0*, December 2001, pp 63. http://www.business2.com/articles/mag/0,1640,35253,FF.html

Sparrow, M.K. 1991.The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13: 251-274.

Sydney Morning Herald. 2001. The hijackers… and how they were connected. September 22. http://www.smh.com.au/news/0109/26/world/

United States Department of Justice. 2001. Indictment of ZACARIAS MOUSSAOUI. December 11. http://www.usdoj.gov/ag/moussaouiindictment.htm

United States Department of Defense. 2001. Transcript of bin Laden Video Tape. December 13. http:// www.defenselink.mil/news/Dec2001/d20011213ubl.pdf

Washington Post. 2001. The Plot: A Web of Connections. September 24. http://www.washington post.com/wp-srv/nation/graphics/attack/investigation_24.html

Watts, D. J. 1999. Networks, dynamics, and the small-world phenomenon. *American Journal of Sociology* 13(2): 493-527.