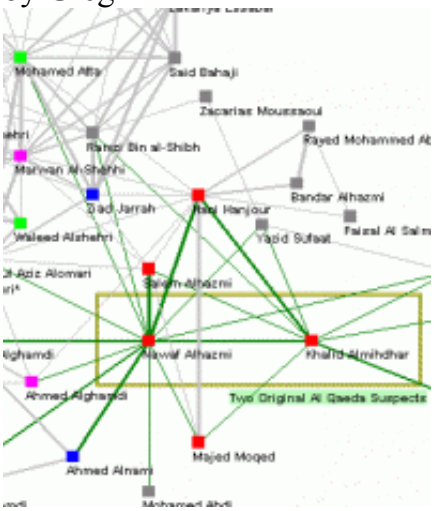
Skip to content

How The NSA Uses Social Network Analysis To Map Terrorist Networks

2013 June 12
tags: Duncan Watts, Network Theory, Privacy, Social Network Analysis, Social Networks
by Greg



Ever since *The Guardian* reported that the National Security Agency (NSA) has been collecting the phone record metadata of millions of Americans, the cable talk circuit has been ablaze with pundits demanding answers to what should be obvious questions.

Who knew about the program to collect data? (Apparently, all three branches of government). Who else has been supplying data? (Just about everybody, according to the *Washington Post*). What is metadata? (It's data about data).

The question that nobody seems to be asking is probably the most important one: What is the NSA doing with the data and why do they need so much of it? The answer is a relatively new field called social network analysis and, while it may make people uneasy, the benefits far outweigh the risks, so it is probably something we will just have to accept.

The New Science of Networks

The story of networks starts in 1736, long before the United States became a country, when Leonhard

Euler set out to conquer a famous math problem concerning the Seven Bridges of Königsberg. To solve it, he created a new form of mathematics called graph theory, which concerned itself with links and nodes in a network.

In the 1950's, interest renewed in Euler's networks. First, Anatol Rapoport introduced the concept of triadic closure, which asserted that networks grow when people meet through a central friend that they both know. Later, Erdős and Rényi showed that as networks got bigger, communication among the people in the ne ch more efficient.

In the 1970's a s med Mark Granovetter argued that we get most of our information not through close fr ough weak ties and in the 1990's Watts and Strogatz built on Granovetter's work by showin clusters of people naturally organize themselves into far flung networks.

So by the late 1 all field of network analysis had built into a full fledged science and it was about to be appl easingly important problem: Terrorist networks.

Mapping Terr ks

Valdis Krebs of etwork scientist who in 2002 published a widely praised paper on mapping terrorist networ ce consulted with the Defense Department on methods and approaches of evaluating and c rrorist organizations.

While he isn't p fied information, he describes on his website how an entire network can be mapped using c available software by identifying two initial suspects:

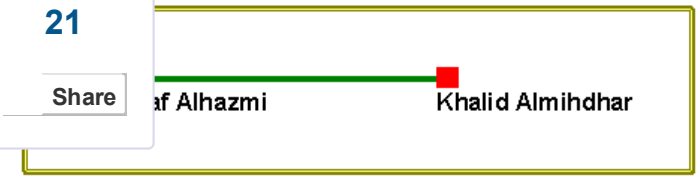


Figure 1 - Two known suspects in January 2000

It used to be that law enforcement officers would simply watch the two men closely, but in the era of global jihad, that's much too slow to save lives. The two might be peripheral to the conspiracy and it could take years before you could connect them to the leadership of the network, if ever.

Here's where the data from Verizon and other companies comes in. If you can analyze communication records, you can move much more quickly. However, you don't want to look at everyone the suspects talk to because you'll end up with mostly incidental contacts, like friendly neighbors and delivery men.

But if you kept Rapoport's concept of triadic closure in mind and had full access to communication records, you could look for contacts the two suspects have in common and start to build out a map of the conspiracy.

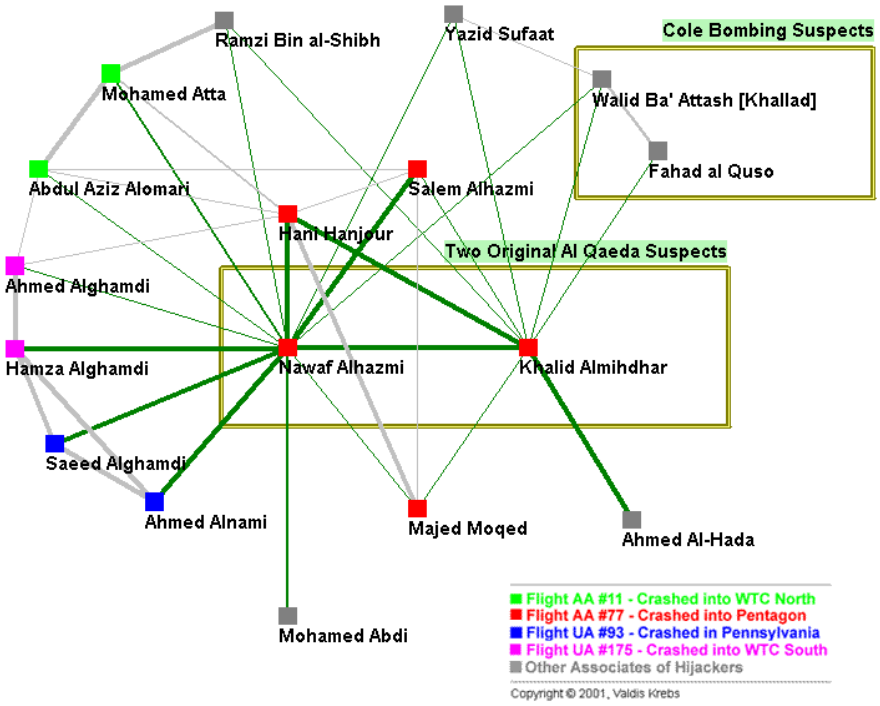


Figure 2 - All nodes within 1 step [direct link] of original suspects

The next step would be to analyze the contacts of the suspects' connections, again looking for closed triads within the existing network. As you progress from link to link, a fuller picture begins to form (click to enlarge).

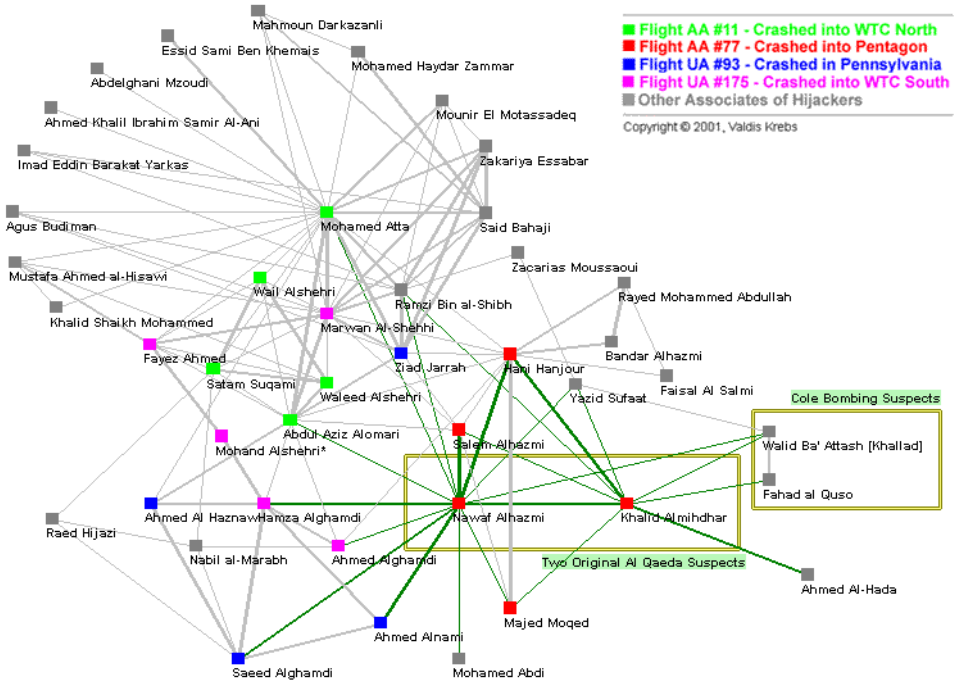


Figure 3 - All Nodes within 2 steps / degrees of original suspects

Once you have the network mapped, you can begin to mathematically analyze it, which is how important insights can be gleaned even before wiretapping and surveillance warrants have been issued.

You can, for example, assess who is well integrated into the network by calculating who is most central; who has the widest reach by counting how many people in the network are within two connections from them and who in the network provides a crucial role as a bridge between otherwise unconnected people (as Mohamed Atta, the uppermost green node, does in the 9-11 network above).

The result is an almost uncannily accurate picture of the leadership, who can then be targeted to dismantle the network. (It has been estimated that the 9-11 network could have been broken up if just three central nodes had been taken out).

Integration		Reach		Connector	
Mohamed Atta	422	Mohamed Atta	28	Mohamed Atta	939
Nawaf Alhazmi	388	Nawaf Alhazmi	26	Ramzi Bin al-Shibh	773
Hani Hanjour	334	Ramzi Bin al-Shibh	24	Nawaf Alhazmi	741
Marwan Al-Shehhi	320	Marwan Al-Shehhi	23	Zacarias Moussaoui	602
Ramzi Bin al-Shibh	310	Hani Hanjour	22	Marwan Al-Shehhi	590

It should be clear by now why the government regards access to communication records as so crucial to national security. If the system had been in place in 2001, there is a high probability that the 9-11

network would have been broken up, saving thousands of lives and trillions of dollars.

It would be impractical, to say the least, to get court orders for each and every connection a suspect has, most of whom would not even be investigated. Without a full data set, the social network analysis could not be done and more intrusive, but less efficient methods, would need to be employed.

So whatever you might think of the program, it is most probably here to stay. What is perhaps of greater concern is that this type of analysis is not unique to antiterrorism, but is increasingly becoming a basic fact of commercial life.

Beyond the cell phone companies, social networks like Facebook, Google+ and Twitter can analyze the communications of hundreds of millions of people. Retail giants like Amazon, Walmart and Target are sifting through our purchases in order to predict our future behavior.

Wherever we go, our movements, faces and actions are being analyzed and, more often than not, it is not the government.

The truth is that there is a dark side to technology and our privacy is being breached every day by someone, somewhere. That's just a fact of modern day life. It seems to me that if we're willing to accept it from marketers who are trying to to sell us goods and services, we should be able to tolerate it from those who are trying to protect us.

– Greg

Note: *Special thanks for Valdis Krebs of Orgnet for supplying the network maps, calculations and consultation for this post.*

Related posts:

How to Approach Social Influence
3 Ways to Use Social Network Analysis for Marketing
The Amazing Possibilities of Social Search
How Social Network Analysis Solves Real World Problems
3 Things You Should Know The Network Economy

from → All Posts, Technology

9 Responses leave one →

1. Alistair McMillan permalink
June 12, 2013

Recently, a news article carried the headline: “Did you really think Google was on your side?” Wrong question. The right one is whether they – or anyone else (government, CIA, google, internet user, whistleblower, whoever) is on the side of according the broader public their rights to freedom, security and is prepared to be sufficiently transparent about any of their activities which may affect another person or group of people. Google is a business; their motive is profit, and as long as they make it legally AND ethically, that’s fine. Government should ensure that the laws and practices of business and their own agencies are ethical, but every government necessarily has secrets – they must have because of the nature of politics. Whether their secrets are sinister (eg. an operation to poison an an outspoken critic) or ethically and morally correct (eg. an operation to covertly uncover a terrorist plot dangerous to thousands of innocent people) is the question. It is not yet a proven fact that any of the information they may have access to has been abused. And what is the big deal about the government having potential access to your personal information when you are not committing a crime and aren’t involved in anything ethically or morally wrong, in the light of the terrorist threat who WILL abuse their rights to freedom, who WILL endanger others’ liberties?

However, I say, while the guy who leaked the info about PRISM hasn’t done the world a great deal of good thereby, he is neither a hero or a villain. I don’t think the National Security agencies are doing themselves or anyone any favors by sticking to their line that he has broken laws and must pay. The fact that they have apparatus in place to secure the US does not need to be secret. The fact that they were conducting surveillance on communications was already widely known, and my guess is that terrorists will simply now find ways to communicate that can’t be tracked, which is a blow to security – but also makes it more difficult for the terror network to operate efficiently.

I think we all need to take a step back, stop throwing tomatoes at each other, and remember who the real enemy is.

[Reply]

Greg Reply:
June 12th, 2013 at 9:19 pm

Alistair,

Some good points. However, I do think there is a problem with the government listening in on private conversations and strongly believe that digital privacy is a very important issue (and wrote about some of the dangers here).

I think the salient point about the NSA program is how restrained and reasonable it is (at least as its been reported). It basically seems to be used to zero in on people whose privacy needs to be violated rather than violating everyone’s privacy in the name of security. It also has congressional and judicial oversight. All in all, it appears that everything is being done by the book.

And that’s what’s important. What you don’t want is a small group of people going off on a flyer and making their own rules. If we don’t like the rules, we can change them. If people are free to break the rules, we truly have no protection.

– Greg

[Reply]

Alistair McMillan Reply:
June 14th, 2013 at 11:52 am

Thanks for the reply Greg. Agreed, we never know which direction a government or agency will take in future, and we need safeguards in place to make sure they don't abuse their power, also agreed that they currently seem to be acting within their mandate.

[Reply]

2. 

Neno permalink
June 14, 2013

is this a re-post?

haven't you post this already?

[Reply]

Greg Reply:
June 14th, 2013 at 8:33 am

It was previously posted on Forbes.com. There is some overlap between my column there and my personal blog and I'm contractually obligated to a short embargo period before I post here.

– Greg

[Reply]

Neno Reply:
June 16th, 2013 at 6:30 am

I was thinking on Krebs' paper.
pretty sure I read it here first.

anyway, doesn't matter.

great post as usual.

keep ‘em coming.

[Reply]

Greg Reply:
June 16th, 2013 at 6:41 am

I think that was an earlier paper. I just spoke to him about this one last week.

In any case, Valdis provides a great, easy to understand overview of social network analysis on his site. If you’re interested in SNA, you should check it out:

http://www.orgnet.com/sna.html

– Greg

3. 

Marco Berrocal permalink
July 23, 2013

This last bit sums it up:

“It seems to me that if we’re willing to accept it from marketers who are trying to to sell us goods and services, we should be able to tolerate it from those who are trying to protect us.”

They are the same scenarios yet people react so harshly towards one.

Well written. I for one, have no problems with it. Having problems with one but not the other is contradictory.

[Reply]

Greg Reply:
July 23rd, 2013 at 9:37 pm

Very true. Personally, I think we should be cautious about both, but not to the point of hysteria.

– Greg

[Reply]

Leave a Reply

Name: (required):

Email: (required):

Website:

Comment:

Note: You can use basic XHTML in your comments. Your email address will **never** be published.

Subscribe to this comment feed via RSS

commentluv

Notify me of followup comments via e-mail

Notify me of follow-up comments via e-mail

Submit Comment

- # Search

type and press enter

- # Follow Me

- # Free Newsletter

Email Address*

First Name

Last Name

* = required field

Subscribe

powered by MailChimp!

- **Related Posts**
  - How to Approach Social Influence
  - 3 Ways to Use Social Network Analysis for Marketing
  - The Amazing Possibilities of Social Search
  - How Social Network Analysis Solves Real World Problems
  - 3 Things You Should Know The Network Economy

- **Recent Posts**
  - The Social Tax: Why Firms That Ignore Social Engagement Pay A Heavy Price
  - Let's Face It, We Don't Really Care About Privacy
  - The Synchronized Organization
  - Could Ukraine Be The Next Silicon Valley?
  - The Truth About Foxcatcher

- **Categories**
  - All Posts
  - Management
  - Marketing
  - Media
  - Technology

- **Featured On**

Vigilance Theme by The Theme Foundry