DE GRUYTER
OPEN

DOI: 10.1515/irsr-2013-0021

IRSR INTERNATIONAL REVIEW of SOCIAL RESEARCH

Volume 3, Issue 3, October 2013, 53-61 International Review of Social Research

Analyzing Behavior Within Networks After Fragmentation. The Coagulant Agent Approach

Tudor RAȚ[•]
University of Bucharest
Department of Sociology

Abstract: This paper introduces a simple mathematical algorithm for identifying the nodes that will most likely act as re-coagulants once the 'key-players' are removed. By comparing the difference between in-degree and out-degree centrality scores (assuming that the relational data are directed) and comparing that value with the overall degree score, one can infer where a node sits on the 'sink-source' continuum. Furthermore, assuming that the nodes will not change their behavior patterns as a result of the prior 'intervention', this algorithm could indicate whether the nodes will act as relational 'magnets' (will attract new ties) or as 'leeches' (will seek to attach themselves to other nodes).

Keywords: *disruption, intelligence, Key Player Problem, network resilience, post-intervention.*

Introduction

Targeting analysis has long been a staple of covert intelligence activities and operations: identifying individuals that are, simultaneously, *valuable* (for example, posses specific assets, can gain access to a hard-to-reach place) and *vulnerable* (faulty character traits such as greed, do not guard professional secrets etc.) is very important in *Human Intelligence* (HUMINT)[1], aiding in planning successful recruitment, infiltration and, last but not least, dismantling strategies that target adversaries.

One particular type of adversary that intelligence organizations face nowadays, after the end of the Cold War, are criminal groups which are fluid, dynamic, resourceful and pose a legitimate threat to nation-states' interests. For example, Romania, a NATO member since 2004, evaluates that the biggest threats today are not military aggressions perpetrated by hostile states, but asymmetric threats such as terrorism and the activity of trans-national crime cartels[2].

In accordance with this paradigmatic change, a shift of perspective has occurred in the intelligence field ever

[•] e-mail: rat.tudor@gmail.com. Tudor Rat works as an Assistant Professor at University of Bucharest, Department of Sociology. He is also a Ph.D. student at University of Bucharest, Doctoral School of Sociology.

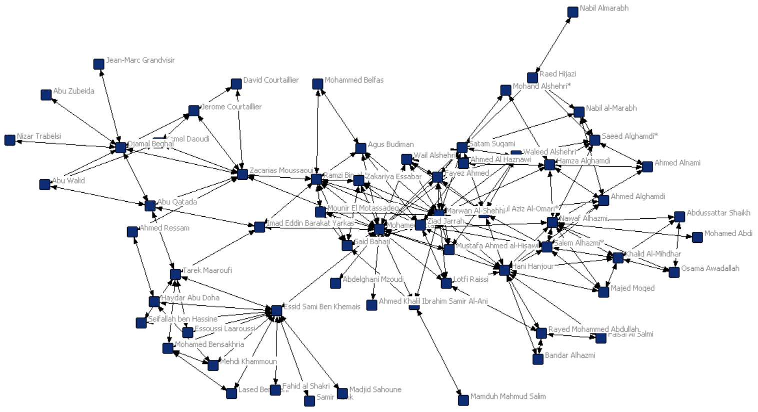


Figure 1. *The network of the al-Qaida group that carried out the attacks against the World Trade Center and the Pentagon on September 11, 2001 (Krebs, 2002).*

since 9/11: such dangerous enemies are not viewed as groups, but as networks, collection of individuals that form ties and, with them, a relational architecture that can be mapped and, more importantly, measured. As such, social network analysis, a profoundly academic domain with a strong interdisciplinary core, has been used by intelligence organizations to perform better targeting analysis that focus on such "dark" networks[3]. Finding the "best-suited" individual is now a matter of careful analysis that often relies on specific metrics and algorithms.

Also in response to the terrorist attacks planned and carried out by al-Qaida in September 2001, a niche in intelligence analysis has been consolidating, that of finding the best way to dismantle terrorist networks by targeting important individuals that, once removed, collapse the relational architecture within the group.

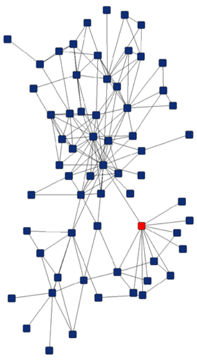
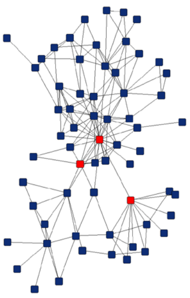
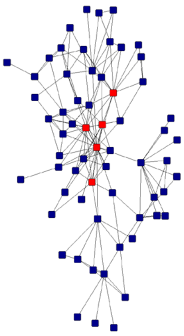
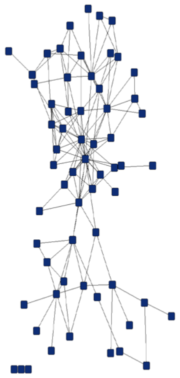
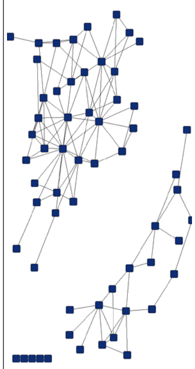
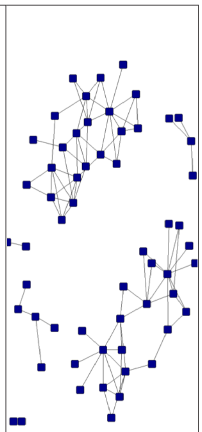
Borgatti's Key Player Model

Borgatti (2003, 2006) built *Key Player* algorithms designed to identify *important* actors in a network from two standpoints. Firstly, entities, that once removed, maximally disrupt the network (*KPP-1* or *KPP-Neg*), by creating breach or, in other words, a decrease of the cohesiveness of the network. Secondly, entities that can be used (e.g. for spreading information) due to their connectedness and embeddedness in their network (*KPP-2* or *KPP-Pos*).

The Key Player Approach takes into account the cumulative effect on the network of removing or using sets of nodes. As such, applying *Key Player 1*, a software tool designed to calculate KPP-1/ Neg and KPP-2/ Pos, to identify variable sized sets, could generate different results based on the size of the group. In other words, KPP-1/ Neg for example, does not simply add the *aftermath* of the removal of each node, but looks at the combined effect of the set of actors (cutset) best fit for extraction. For the purpose of this paper, I will focus on the KPP-1/ Neg algorithm.

Analyzing the 9/11 Krebs' Terrorist Network using Key Player 1

Applying the Borgatti's KPP-1/ Neg algorithm to the Krebs' relational data describing the Al-Queda dark network, one might obtain the following results (Figure 2).

Size of node set	1	3	5
Actors identified	Essid Sami Ben Khemais	Mohamed Atta Ramzi Bin al-Shibh Essid Sami Ben Khemais	Hani Hanjour Mohamed Atta Marwan Al-Shehhi Ziad Jarrah Ramzi Bin al-Shibh
Position in the network			
Fragmentation*	0.124	0.590	0.662
Generated breach	3 isolates	2 components, 5 isolates	5 components, 2 isolates
Visual results**			

*Proportion of the network affected by the removal of the node set.

**The disconnected network was visualized after using the Net Draw software package

Possible limitations within Borgatti's model

Although Borgatti's KPP-1/ Neg is a useful instrument for aiding intelligence analysis in identifying best cut sets, it serves limited purposes. Given the fact that the software solution is based on a mathematical algorithm, (intelligence) analysts must be aware of the limitations of such an approach.

There are at least four possible limitations within Borgatti's Key Player model. The first one refers to the *data quality*. Data collection on dark networks is always problematic and, consequently, missing data greatly decrease the effectiveness of the KPP-1/ Neg metrics.

The second one refers to the problem of *trajectory.* This means that the approach is centered on the geodesic (shortest) path between two nodes, taking into account the distance between actors as to identify the sets of nodes that could maximally impact the network by disconnecting it. Although it is theorized that information flows through the shortest path in a network, other social processes follow different trajectories (e.g. gossip could travel unrestricted across nodes and ties, along walks in the network).

The third possible limitation refers to the problem of *the tie value*. Put it differently, the algorithm works only on undirected graphs ('a,b' is identical to 'b,a') with non-valued edges (ties are not-valued).

The last possible limitation of the model refers to the *node attributes*. In a dark network, members often have different types of attributes that complement each other and work in symbiosis (e.g. a bomb maker needs a supplier of explosive material, which in turn needs a person to finance the purchase)[4].

Robins and Kashima (2008) and Robins (2009) have argued that not taking into account attributes of actors only paints an incomplete image and may lead to incorrect targeting, while Xu and Chen (2007), Keegan, Ahmed, Williams, Srivastava, and Contractor (2010), Sageman (2004a, 2004b) and Everton (2012) argue that more factors must be taken into account when identifying the key players of a network.

The latter argue that most dark networks display a "scale-free" (Barabasi, 2002; Barabasi & Bonabeau, 2003) architecture: most nodes have few connections, while some have a large number of connections. A property of a scale free network is that, although it is resistant to *random* attacks (e.g. removing a node from a network by arresting that individual), the network collapses under targeted, simultaneous attacks against the *hubs* (the well connected nodes). As such, more and more complex algorithms have been proposed as solutions of dismantling or destabilizing dark networks (Carley, Lee & Krackhardt, 2002; Carley, Reminga & Kamneva, 2003; Carley, 2006; Bright, Greenhil & Levenkova, 2011).

A matter of strategic choice

Besides the limits of Borgatti's model, I consider that the subject of dismantling dark networks to be extremely nuanced. Although a layman's approach would call for dismantling all the dark networks encountered, the intelligence approach to different types of groups greatly varies. While terrorist networks are prosecuted to the fullest capabilities of intelligence and law enforcement agencies, other networks are not "disturbed" for long periods of time.

For example, espionage networks are seldom broken apart by intelligence organizations. Such an approach would *tip the hand* and cause the adversary to change its tactics and strategies. Catching a *spy* and expelling that individual would cause a mirrored reaction on the part of the state in the name of which the spy carried the illegal intelligence activity.

Another type of case in which removal of an important actor would cause more harm than good in the long run is that of drug smuggling organizations. Arresting a leader would cause a power void and generate power struggles, often violent processes both within the organization and among competitors.

Although targeting individuals that could, once removed, generate fragmentation in the network is not an easy analytic endeavor, the discussion becomes even more complex when it comes to other ways of reducing the operational capacity of a dark network. For example, eliminating Osama bin Laden had no direct impact on Al-Queda, as he was hiding ever since 9/11 and was only communicating with a small circle of top-tier leadership. Especially in the short term, his removal caused no effect on a tactical level. On the other hand, he had a significant symbolic and ideological value for the organization.

In other words, fragmentation potential only tells a partial story of the importance of a node in a particular network. The downside is that *importance* is a diffusive concept, which can be operationalized through a number of social network analysis metrics and algorithms.

For the purpose of this paper I will not go into great detail over the various metrics that can be used to quantitatively and qualitatively evaluate the position of a node in a network. Centrality measures (e.g. degree, closeness, betweenness, eigenvector), structural hole index, E-I Index, K-core score, Ego Network Density score are but a few examples of algorithms that show different facets of node *importance*.

The Post - Key Player Problem

Given the fact that networks are dynamic and fluid in their nature, this type of structures display emergence: they act and react to changes in the environment. Changing the *natural* equilibrium might generate *unexpected effects* such as *spillover, change of architecture, change of modus vivendi, loss of negociation capability*.

The Spillover effect

In early 2012, the Tuaregs in northern Mali attacked government forces with the purpose of attaining independence for the region known as *Azawad*. The National Movement for the Liberation of Azawad (MLNA), the insurgent organization, featured a significant number of Tuareg mercenaries that fought in the Lybian Civil War, alongside Muamar Gaddafi[5]. The ousting and subsequent killing of the former dictator dislodged significant manpower and armament from Libya and generated processes in Mali.

The Change of Architecture effect

Braffman and Beckstrom (2006) argue that removal of key players from structures that are decentralized by nature (such as terrorist groups) would only cause them to become more decentralized.

The Change of Modus Operandi effect

Sageman (2008) argues that the pressure put by US and NATO states on al-Qaida and other terrorist groups have "helped" spawn a new era of a "leaderless jihad" – amorphous movements that are hard to track and combat.

The Loss of Negotiation Capability effect

According to Gourley et al. (2009), an increase of operational aggressiveness on the part of government organizations might successfully impact terrorist architectures. In Iraq, for example, the tactical victories of the coalition forces from 2003 onward destabilized the insurgency ecology and caused fragmentation (more groups, but weaker). The downside of this approach is that there are no significant actors who could broker a peace deal between the insurgents and the government.

To sum up, an intelligence analyst must decide if intervention in the direction of dismantling a dark network is the adequate choice in the long run, not just for the immediate future.

The Coagulant Agent approach

Tsvetovat & Carley (2005) found that terrorist networks are resilient and self-healing, properties that are characteristic of scale-free networks. As such, dark networks display super-organism qualities: they adapt, transform, heal and, quite often, fight back aggressors. It means that, once dismantled, networks do not remain broken, they coalesce, re-connect, or seek new *umbrella* organisations. As such, the Post-Key Player problem could be as important as the original problem suggested by Borgatti (2003).

In line with the demonstrated predictive capacity associated with social network analysis metrics, I believe that coagulant agents (i.e. nodes that act as agents of reconnection, either between former connected components, or between newly disconnected components and similar organizations) could be identified by analyzing their relational architecture[6].

Given a directed graph, all nodes occupy a certain position on the sink-source continuum. A *sink node* is a node that only *receives* ties. It has an out-degree of 0 and an in-degree equal to or larger than 1. A *source node* is a node that only *sends* ties. It has an in-degree of 0, and an out-degree equal to or larger than 1.

Given a directed graph G (V, A), the *Magnet-Leech Score* (*MLs*) can be calculated by dividing the difference between out-degree and in-degree centrality to the overall degree centrality score (where a *leech node* would be a point that has an out-degree higher than the in-degree, while a *magnet node* would be a

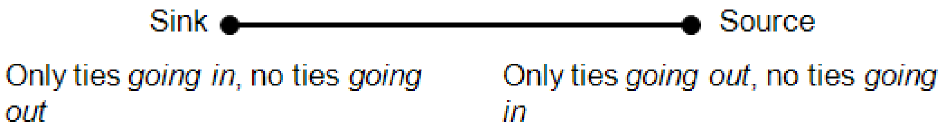

Sink
Source
Only ties *going in*, no ties *going out*
Only ties *going out*, no ties *going in*

Figure 2. *The Sink-Source continuum, where each node of a specific network could be placed*

vertex with higher in-degree than out-degree). Computing *MLs*, by the below formula, each node potentially could be assigned a score between '-1' (i.e. a sink node) and '+1' (i.e. a source node).

$$MLs \;=\; \frac{deg^{+}(v)-deg^{-}(v)}{deg(v)}$$

The compatibility conjecture

Assuming that relational patterns hold post-dismantling, leeches and magnets will likely *seek* each other out (see disconnected directed tie in Figure 3).

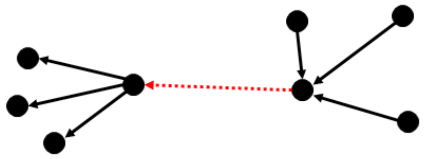


Figure 3. *Post-dismantling behavior of nodes within a given network*

As such, the conjecture proposed in this paper is that symmetrically positioned nodes on the sink-source continuum display maximum compatibility (In Figure 4, zero stands as a median point on the interval and indicates neutrality).

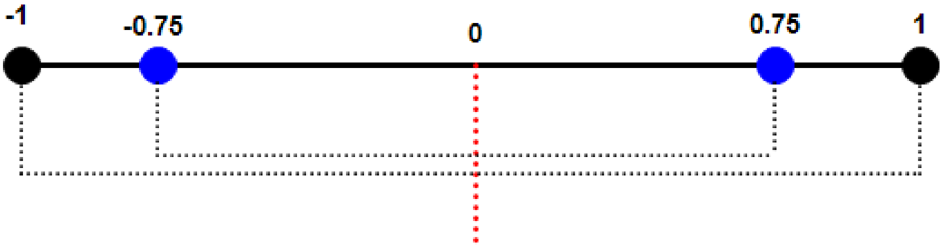


Figure 4. *Symmetrically positioned nodes on the sink-source continuum display maximum matching*

Limitations within the coagulant agent approach

The coagulant agent approach contains several limitations. First of all, MLs formula is applicable only to directed networks (i.e. within undirected graphs, each node would get a MLs of zero regardless of the degree). Second of all, ties must support resource circulation (e.g. 'A' transfers money to 'B', 'X' visits 'Z' etc.). Third of all, the problem of *isolate idleness* cannot be solved with this approach. In other words, if a network has isolate nodes pre-dismantling, then the stressor of intervention could affect the relational pattern of that particular node. There is a theoretical possibility for the isolates to become active. And if they become active, there is no knowledge about their propensity to act as magnets or as leeches. A last limitation of the approach refers to the role-based behavior, that it is not taken into account (this approach ignores attribute data).

This algorithm could be empirically tested in the field of intelligence practice, but ethical and obvious practical reasons make such testing an utopian goal.

Notes

[1] A specific type of intelligence obtained from humans, through interpersonal contact (e.g. source-handler relation). See http://www.princeton.edu/~achaney/tmve/wiki100k/docs/HUMINT.html Retrieved: October 20, 2013.

[2] See National Defense Strategy (2010), available at: http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf. Retrieved: October 20, 2013.

[3] Defined by Raab and Milward (2003) as groups of individuals that perform actions that are, simultaneously, illegal and covert.

[4] Carlo Morselli's *Project Ciel* case-study is a detailed example of how dark networks are sometimes organized as collaborative architectures (2009: 51-60).

[5] See http://thinkafricapress.com/mali/causes-uprising-northern-mali-tuareg Retrieved: February 6, 2012.

[6] The research on this subject is quite extensive. A good starting point would be Cooke (2006) and Kim, Tang, Anderson & Mascolo (2012), papers that prove causality between the network position of a node and future actions/ potential of a node.

References

Borgatti, S.P. (2003) 'The Key Player Problem'. In Breiger, R. , K. Carley, and P. Pattison (eds.) *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers*, pp. 241-252. National Academy of Sciences Press.

Borgatti, S.P. (2006) 'Identifying sets of key players in a network'. *Computational, Mathematical and Organizational Theory*, 12(1): 21-34.

Carley, K. M. (2006) 'Destabilization of Covert Networks'. *Computational and Mathematical Organization Theory,* 12(1): 51-66.

Carley, K. M., J. Lee and D. Krackhardt (2002) 'Destabilizing Networks'. *Connections*, 24(3): 79- 92.

Carley, K. M., J. Reminga and N. Kamneva (2003) 'Destabilizing Terrorist Networks', http://repository.cmu.edu/cgi/viewcontent.cgi?article=1031&context=isr. Retrived: August 26, 2013.

Cooke, R.J.E. (2006) *Link Prediction and Link Detection in Sequences of Large Social Networks Using Temporal and Local.* Department of Computer Science: University of Cape Town.

Everton, S. (2013) *Disrupting Dark Networks*. Cambridge: Cambridge University Press.

Gourley, S., J. C. Bohorquez, A. Dixon, M. Spagat and N. Johnson (2009)

‘Common Ecology Quantifies Human Insurgency’. *Nature* 462(15): 911-914.
Keegan, B., M.A. Ahmed, D. Williams, J. Srivastava and N. Contractor (2010) ‘Dark Gold: Statistical Properties of Clandestine Networks in Massively Multiplayer Online Games’, http://129.105.161.80/uploads/darkgold.pdf. Retrieved: August 26, 2013.
Kim, H., J. Tang, R. Anderson and C. Mascolo (2012) ‘Centrality Prediction in Dynamic Human Contact Networks*’. Compute,* 56(3): 983-996.
Krebs, V. (2002) ‘Mapping Networks of Terrorist Cells’. *Connections,* 24(3): 43-52.
Morselli, C. (2009) *Inside Criminal Networks*. New York: Springer.
Raab, J. and B. Milward (2003) ‘Dark Networks as Problems’. *Journal of Public Administration Research and Theory*, 13(4): 413-439.
Robins, G. and Y. Kashima (2008) ‘Social Psychology and Social Networks: Individuals and Social Systems’. *Asian Journal of Social Psychology,* 1: 1–12.
Robins, G. (2009) ‘Understanding Individual Behaviors Within Covert Networks: The Interplay of Individual Qualities, Psychological Predispositions, and Network Effects in Trends’, http://link.springer.com/content/pdf/10.1007/s12117-008-9059-4.pdf. (Retrieved: August 26, 2013).
Sageman, M. (2004) ‘Statement to the National Commission on Terrorist Attacks Upon the United States’, http://www.9-11commission.gov/hearings/hearing3/witness_sageman.htm. (Retrieved: August 26,2013).
Sageman, M. (2004) *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.
Sageman, M. (2008) *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press.
Tsvetovat, M. and K.M. Carley (2005) ‘Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence’, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1034&context=isr. (Retrieved: August 26, 2013).
Xu, J. and H. Chen (2009) ‘Untangling Criminal Networks: A Case Study Intelligence and Security Informatics’, http://link.springer.com/chapter/10.1007%2F3-540-44853-5_18. (Retrieved: August 26, 2013).