

Fighting Irregulars

The Critical Role of Network Science

Roy Lindelauf

Most scholars agree that in order to get a grip on the future one should have a clear understanding of the past. It therefore comes as no surprise that many, if not most, analyses of the current wave of international terrorist and insurgent networks are set in historical and political-scientific terminology. Next to this important mode of analysis, however, a fully different field of science, aiming at understanding the nature of networks, has evolved over the past decades. This article sheds light on some of the insights that network science offers when applied to the study of networked organisations that are of a covert nature.

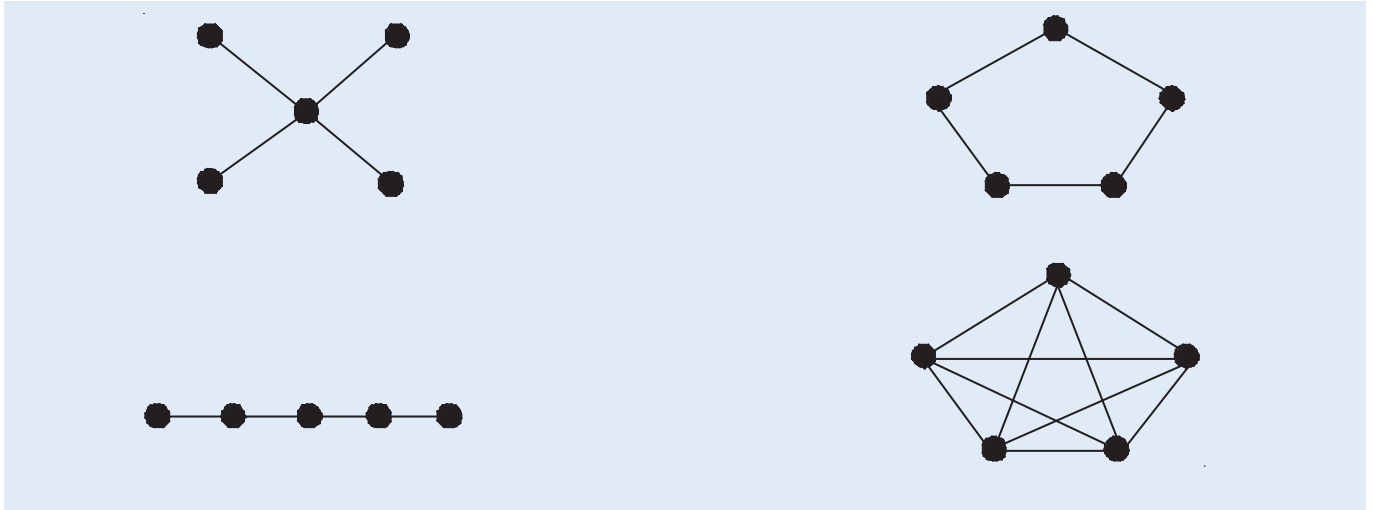
In particular, we will focus on the influence of secrecy on the covert network topology and the identification of key players and its relationship with robustness of networks.

As the Mumbai attack of 26 November showed, modern technology acts as an enabler and force multiplier for terrorists. Tactical commanders and individual team members used satellite and cellphones to connect to strategic commanders out of theatre. Multiple teams consisting of several individuals were able to communicate and direct each other as the attacks progressed. What sets apart such attacks, however, is not the use of technology *per se*; it is the networked mode of operation that enables the technology. The organisational form of these attackers is not easily characterised as being 'hierarchical' or 'decentralised'. However, it is clear that terrorist, insurgent and criminal organisations are increasingly able to cross borders, engage in fluent relationships and 'swarm' their objectives to achieve their goals. The underlying mechanism to all these operations is the networked topology: information is being exchanged via communication networks; weapons diffuse through trafficking networks; and Shura councils meet in affiliation networks. Clearly, these actors and their actions should be viewed as interdependent rather than independent, autonomous units. This also holds true for the amalgam of opponents in Afghanistan that confront ISAF and Operation Enduring Freedom today, be they insurgents, warlords, drug dealers or simply local populace armed with AK-47s.

*The covert
organisation's
challenge is to
reconcile efficiency
and secrecy*

The current conflict in Afghanistan shows that fighting the Taliban and pinpointing Al-Qaeda prime requires, among others, special operations and excellent intelligence. It is the availability of such superior intelligence that sets apart the Taliban from coalition forces: the Tali-

ban are familiar with the terrain and have a big network of supporters. Intelligence focused at understanding the effects of this operational environment and evaluating the threat thus becomes important in fighting such irregulars, a fact recognised by the U.S. counterinsurgency doctrine.¹ To better understand insurgencies in general one should inquire about the impact of its social structure.² As this article will show, network science is the methodology to map such a complex social infrastructure, and can complement the more traditional modes of analysis in understanding the insurgent opponent.



Networks Everywhere

Sociologists recognise that when studying a group of people three key structural components play a role: norms, roles, and relations.³ These aspects are concretised by the stable pattern of relationships that individuals engage in and can be visualised by a collection of nodes connected through links. Thus, nodes represent individuals and links represent the interaction among them. All kinds of interactions can be represented by links, for instance the smuggling of weapons, the exchange of target-selection information, or simply telephone calls. To capture all these diverse interactions methodologically a whole apparatus of network analysis has been developed. It is not uncommon to see directed or undirected links (for instance indicating the sender and recipient of a message); links having weights attached (representing the amount of weapons that are being transferred); and the modelling of probabilistic aspects to incorporate that the information upon which the link is inferred might be uncertain (e.g. due to the reliability of the source of information). Now, having in mind this network science perspective on fighting irregular opponents we will delineate several distinct areas of this broad field of research that can contribute to counterterrorism and counterinsurgency.

Understanding Covert Network Topologies

Different perspectives exist on the structure of groups engaged in the worldwide religious revivalist movement.⁴ For instance: can Al-Qaeda be considered a corporation, a franchise organisation, or an ideological movement? In answering this question, most analysts nowadays would tick the 'all of the above' box. Al-Qaeda's core leadership, mainly operating from the Pakistani Northwest Frontier Province region, is reduced in size and only performs a peripheral function with regard to day-to-day operations. However, its franchise movements ranging from Indonesia, Yemen, the Maghreb and Europe are still active in the formation of underground cells.⁵ Researchers Arquilla and Ronfeldt argue that the basic organisational forms most commonly observed in such networked organisations are the chain network in smuggling op-

erations, the star network found in cartels, and the all-to-all network in e.g. militant peace groups (see figure).⁶ Clearly, hybrid networks that are a mix of these basic networks can and will also be found in real-world networked organisations. The big question becomes what network topologies covert organisations such as Al-Qaeda or Hizbolah's underground wing adopt and why.

This question can be analysed by considering the critical dilemma such organisations have to solve: how to efficiently coordinate and control while at the same time remaining secret. Clearly, such considerations are essential for any underground organisation. For instance, if an underground network would be structured as an all-to-all network (that is: everybody knows everybody else in the organisation), the security risk to the organisation would be very high. The exposure of an individual in the network, e.g. by capture and interrogation, could potentially expose the whole organisation – a risk few organisations would be willing to take. On the other hand, an organisational topology that is very sparsely connected could become impossible to coordinate and control, simply because efficient communication between individuals in such an organisation is very hard. Therefore, some middle ground has to be found.

This dilemma has been analysed from a game theoretical and graph theoretical perspective. Game theory has been used because it is the mathematical theory of strategic interaction between actors, i.e. it can be used to model terrorists and insurgent's incentives and choices of strategies. Graph theory has been applied because it is a well-developed mathematical field solely concerned with understanding the network topology.

Mathematical measures have been developed by which the secrecy and information processing capability of a network could be quantified.⁷ Next, game theoretical bargaining theory has been used to analyse the trade-off between secrecy and information, and a criterion for network optimality has been derived. Finally, given several different scenarios, optimal networks have been analysed.

Nodes represent individuals and links represent the interaction among them. A star network (top left), chain (bottom left), ring (top right) and all-to-all (bottom right).

One of the findings showed that if the probability of detection of all individuals in the network is equal for all individuals, and upon exposure of an individual all his neighbours in the network will be exposed, the star network would be the best organisational form in balancing the trade-off between secrecy and information. However, a star network poses the problem that the central node is the critical one, in the sense that his exposure would expose the entire organisation. Initially, the probability of exposure of the individual corresponding to the centre of a star would equal that of all other members. However, as time progresses this probability of exposure will increase. Therefore, in another scenario, it was argued that a node that is more central to the exchange of information has a far higher probability of being detected. Analysis of this scenario showed that cellular network structures emerge: topologies similar to those found in the current qualitative literature on Al-Qaeda's organisational form.

Clearly, such abstract models are a simplification of a very complex reality. Therefore one should be careful in interpreting these results. However, mathematical models of covert networks do provide insights in the structure of insurgent and terrorist networks. These models provide an objective framework for testing hypotheses relevant to counterterrorism and counterinsurgency. In addition, such models provide baseline metrics that can aid in the search for terrorist cells in large, uncertain data structures.

The Identification of Key Leaders

Traditional social network analysis methodology focuses on questions of centrality: who are the key players in the network? A plethora of measures have been developed to answer this question; both from a mathematical as well as from a sociological viewpoint.⁸ The application of such centrality measures in particular, and network theory in general, is only useful if the practitioner and the theorist are on an equal footing. The methodologist has to ground his theory in observable facts based on intimate knowledge of the social environment he is modelling. He can come by this only when working closely with those having 'boots on the ground'. Vice versa, the practitioner can hugely benefit from insights obtained by methodologically analysing carefully constructed databases reflecting the social complexity at hand. It can help him to more efficiently and effectively find and eliminate enemy groups in his area of operations.



Robustness

The reason to identify key players in a network is obvious: it enables the development of strategies to counter such networks by the isolation or elimination of those critical individuals and groups. However, before such a strategy is being applied one might wonder about the exact effect of such an action on the functioning of the network. This aspect of networks has been studied under the header of 'robustness'. For instance: if we have information or disease propagating through a network, how robust is this propagation to failure or removal of vertices? The relevance of this question to a counterinsurgency campaign may be clear: one wants to affect the social structure in such a way to provide sustained security for the population. In other words: one wants to make sure that the different paths by which insurgents spread fear among the population are being reduced as much as possible by carefully selecting and isolating nodes in the network, similar to the reduction of epidemics by immunisation against the spreading of a disease.⁹

A robustness analysis of a network thus teaches us how the network is being influenced by the removal or isolation of a certain fraction of its vertices. It is argued, for instance, that the diameter is a good measure to model the worst-case performance with regard to the capacity of a network to pass information around.¹⁰ In essence, the diameter of a network is the maximum number of individuals the information has to be passed along to go from source to target. One can analyse how the diameter of a network changes depending on the fraction of individuals that is being removed, and the way in which these individuals are being removed.

In Conclusion

Network analysis complements the more traditional modes of analysis in counterterrorism and counterinsurgency campaigns. It can help us to obtain a good picture of the population; how it is being put together; and more importantly: it can help predict what the likely effect of our deliberate actions will be. One of the most effective weapons against an armed insurgency is good intelligence, as it is recognised that the process of developing background information into contact information constitutes the basic function of counterinsurgency operations.¹¹ Given that intellect is the well from which all good analysis flows, it is paramount that science play an important role in this process in such a way that fighting and defeating the irregular opponent becomes more likely. Clearly, network science alone cannot do that job. However, it will certainly provide a valuable contribution.

Roy Lindelauf works as a researcher and lecturer at the section Military Operational Art & Science of the Netherlands Defence Academy in Breda. At Tilburg University's department of Econometrics and Operations Research he is conducting his PhD research in developing mathematical methods to analyse terrorist, criminal and insurgent networks. In particular, his research focuses on the use of game theory and graph theory to identify covert network structures, identify good destabilisation strategies, and develop models that can support decision-makers in an uncertain environment.

Would you like to react? Mail the editor at info@atlcom.nl.

1. *The U.S. Army/Marine Corps Counterinsurgency Field Manual*, University of Chicago Press, 2007.
2. B.E. O'Neill, *Insurgency & Terrorism: Inside Modern Revolutionary Warfare*, Brassey's Inc., 1990.
3. D.R. Forsyth, *Group Dynamics*, Wadsworth Publishing; 3rd ed., 1998.
4. S. Mishal, M. Rosenthal, 'Al-Qaeda as a Dune Organisation: Toward a Typology of Islamic Terrorist Organisations', *Studies in Conflict and Terrorism* 28 (4), pp. 275-293.

5. L. Vidino, 'Current Trends in Jihadi Networks in Europe', *Terrorism Monitor* 5 (20), 2007, pp. 8-11.
6. J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy*, RAND Institute, 2001.
7. R.H.A. Lindelauf, P.E.M. Borm, H.J.M. Hamers, 'The Influence of Secrecy on the Communication Structure of Covert Networks', *Social Networks*, to appear 2009.
8. S. Wasserman, K. Faust, *Social Network Analysis: Methods and Applications*, Cambridge University Press, 1994.
9. F. Ball et al., 'Epidemics with Two Levels of Mixing', *The Annals of Applied Probability*, Vol 7 (1), 1997, pp. 46-89.
10. F.R.K. Chung, 'Diameters of Graphs: Old Problems and New Results', *Congressus Numerantium* 60, 1987, pp. 295-317.
11. F. Kitson, *Low Intensity Operations: Subversion, Insurgency and Peacekeeping*, Harrisburg PA: Stackpole Books, 1971.

To learn more about network science, have a look at the following information:

Network analysis:

- U. Brandes, Th. Erlebach (eds.), *Network Analysis*, Berlin: Springer, 2005
- S. Wasserman, K. Faust, *Social Network Analysis: Methods and Applications*, Cambridge University Press, 1994

Secrecy versus information dilemma:

- R.H.A. Lindelauf, I. Blankers et al., 'On the Optimal Distribution of Risk and Information Exchange in Star Networks', in: V.S. Subramanian, A. Kruglanski (eds.), *Proceedings of the 2nd International Conference on Computational Cultural Dynamics (ICCCD 2008)*, Los Alamitos: IEEE, 2008, pp. 45-48
- R. Lindelauf, P.E.M. Borm, H.J.M. Hamers, 'Mathematical Methods in Counter-terrorism', in: N. Memon, J.D. Farley et al. (eds.), *On Heterogeneous Covert Networks*, Springer-Verlag, to appear August 2009