MARTIN EVERETT

COVERT NETWORKS

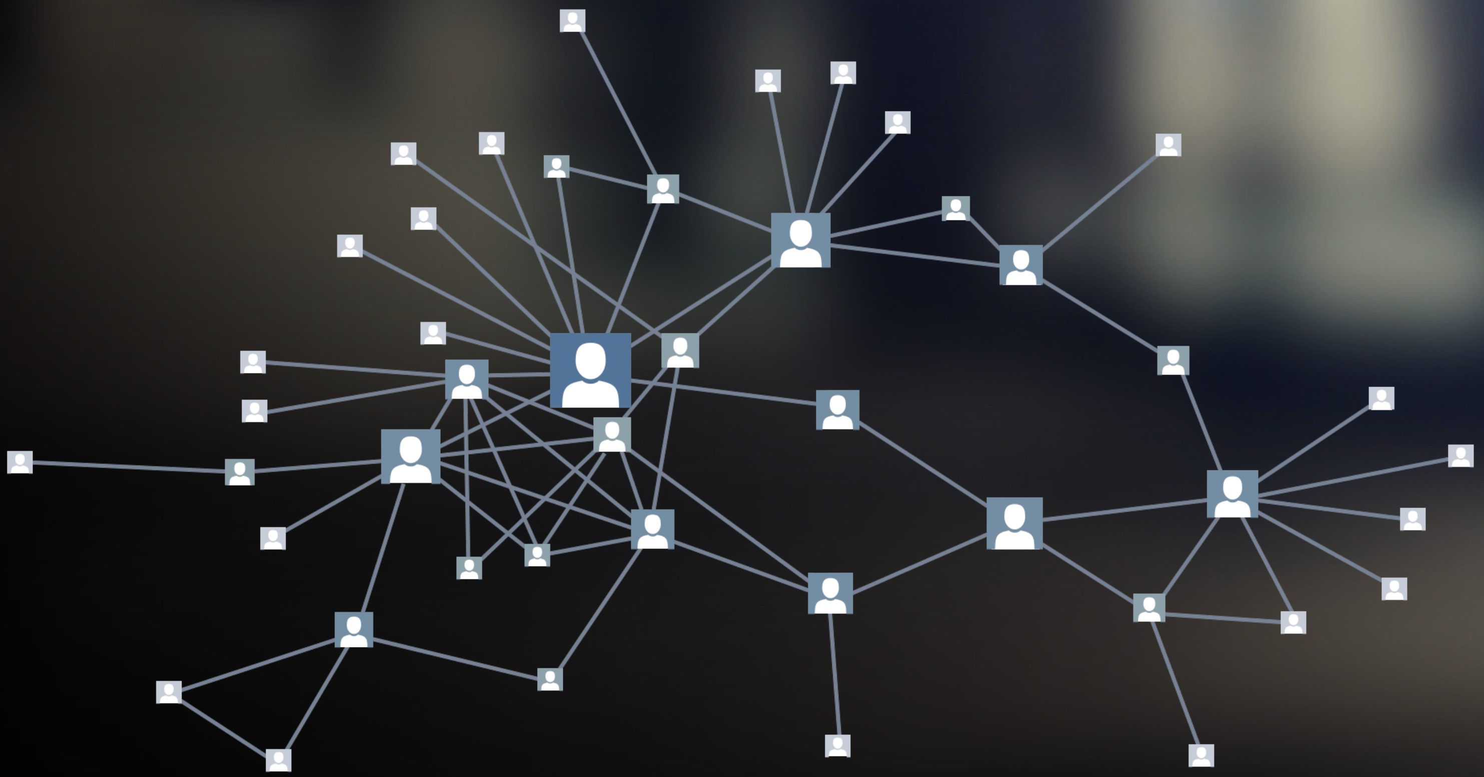
How can social network analysis help with the study of terrorist and criminal networks? Martin Everett researches covert, or dark, networks and presents an example based on the Provisional Irish Republican Army (PIRA).

Social networks are a way of thinking about social systems that focus on the relationships among the entities that make up the system, these entities can be people or collectives such as organisations, or families, and are referred to as actors or nodes. The nodes often have characteristics – typically called 'attributes' – and these can be categorical traits, such as having a conviction, or continuous attributes, such as being 52 years of age. The relationships connecting the nodes can be of many different types and each relation gives rise to a separate network. Examples of relationships are 'friendship', 'talks to', 'associates with', as well as secondary types of tie such as 'arrested with', 'attended the same church as', 'belonged to the same club as'.

As an example of a network, the diagram below is the main connected portion of part of the PIRA. The nodes are known PIRA members and the relations are one or more of the following: 'took part in an active mission', 'were friends before joining', 'are blood related directly' or 'are related by marriage'.

Data in this case was obtained from a variety of accounts and historical documents. In other examples data has been obtained from wire taps, via co-arrest and co-offending or from public sources. A collection of publically available networks that describes the data and how it was sourced is available at: *https://sites.google.com/site/ucinetsoftware/datasets/covert-networks*

Once the data is in network form an analyst has a number of tools that can be used to help uncover important features. A simple visualisation of the data is often helpful in identifying portions of the network of interest.



For example, nodes with a high number of connections could well indicate a level of activity consistent with a co-ordination or leadership role.

One consistent finding in social network research has been that people tend to associate with people like themselves. This includes criminal and terrorist actors, and so if we have a known criminal or terrorist in a network it would be worth looking closely at who they are connected to because those may be the most likely to be involved in similar offending. This approach has been successfully applied to fraud networks.

There are a number of techniques used by analysts to uncover important properties of the network. Two are particularly important. The first is to identify actors who occupy structurally important positions. As already discussed, looking for nodes with a large number of connections is one such example. A subtler example is to identify nodes who are well placed to capitalise on any information flowing through the network. This is called betweenness centrality and in our diagram I have sized the nodes proportionally to this measure. In real life applications, including this example, such nodes are often those in leadership positions and so network analysis can help determine on which actors to target resources.

A second useful technique is to identify portions of the network in which actors are more closely associated with each other than with other actors. Such portions are called cohesive subgroups or communities. This is important as offending tends to be organised in clusters, so identifying the clusters in the network again allows resources to be targeted.

Professor Martin Everett
Mitchell Centre for Social Network Analysis, University of Manchester