Seminar Series Session 03 - Meeting Minutes

Topic: Structured Analytic Techniques - Actor and Network Analysis
Format: Expert Talk
Experts: Mr Randolph H. Pherson (Globalytica), Ms Cynthia Storer (Johns Hopkins University), Ms Monika Rückert (Joint Forces Operations Command German Armed Forces), Viviana De Annuntiis (NATO Joint Forces Command Naples)
Moderators: Major Ralf Baur, Mr Nathanael Ott
Date: 04 Mar 21, 15:00 UTC+1
Duration: 120 min

Agenda:

Part 1: Mr Randolph H. Pherson - Introduction to Actor and Network Analysis

Part 2: Practitioners' Brief
a. Ms Cindy Storer - Best Practices from The Discovery of Al-Qaeda
b. Ms Monika Rückert - Network Analysis - A Practical Approach
c. Ms Viviana De Annuntiis - Actor Analysis in The Western Balkans

Guiding Questions:

1. What are strengths, weaknesses, and limitations of actor and network analysis?
2. How and in what contexts should actor and network analysis be applied?
3. What potential pitfalls do practitioners face when conducting actor and network analysis, and how to respond to those challenges?

Part 1: Mr Randolph H. Pherson - Introduction to a Structured Analytic Technique - Actor/Network Analysis

Broad overview of Network Analysis and Link Analysis in 2 steps:
- What is it?
- How do we use it?

What is (Social) Network Analysis?
- Network Analysis has become a robust science in itself
- In essence, one is trying to map and measure relationships to reveal patterns between people
- Understanding patterns and uncovering key actors in networks improves overall analysis efforts and supports decision-making for targeted measures and resource allocation

→ Network Analysis has become an essential tool and many organisations have developed their own software

In Intelligence:

- Network Analysis maps an entire network and allows the analyst to visually track it and to deduct assessments based on its structural properties
- I.e., one can follow the lines to see who is in contact with whom, and make assessments about how and by whom decisions are processed and executed in the network.

Mapping a Network

1. Identify the nodes. Nodes of a network are usually relevant individuals.
2. Draw linkages between the nodes to show how they relate to each other. This can be done with simple lines or arrows. The guiding questions are: Who is talking to whom, what is going on?

Once a network is established, one can look at the relative position of the nodes and their relationships in more detail. Mr Pherson presented three ways to assess the position of a node:

- Degree Centrality
    - Measures the number of direct connections a node has
    - Individuals with many connections act as “connectors” in the respective networks

- Betweenness Centrality
    - Describes nodes that connect otherwise unconnected nodes - these individuals are called “bridges”
    - Bridges may have the power to decide who talks to whom. It is important to identify the role of the individuals involved (e.g., does a node connect the branch chief to a working group). They may act as gatekeepers with regard to the flow of information in a network.

- Closeness Centrality
    - Describes who has the shortest path to everyone else in the network
    - Individuals with the shortest path can be assumed to be influential within the network, as they have a privileged access time to information.

Describing a Network

- Centralized Networks
    - hub and spokes, e.g. Al-Qaeda
- Less Centralized Networks
    - no single point of failure, e.g. Antifa in US
- Horizons of Networks
    - usually, information & resource flow diminishes after a few steps
- Boundary Spanners
    - move between different networks with different group cultures
    - ‘translate’ knowledge from one group to another
    - connect otherwise separate groups

Example: 9/11 Hijackers
Mr Pherson illustrated his theoretical discussion with the example of the 9/11 hijackers:

Approach:

- identification of
    - Length of connection, how many steps lay between two individuals?
    - Bridges
    - Centre of the network: Who scores high at degrees of centrality?
    - Subgroups, cliques
- broader network of accomplices shows different smaller networks connected by boundary spanners
- Network Analysis gave crucial insights into what was happening, who should be targeted by identifying key nodes of the network.
- Conclusions:
    - the network of hijackers was sparse, they were relatively isolated, connections long
    - monitoring meetings allowed analysts to identify shortcuts in the networks' lines of communication and uncover the clique of pilots
    - their activity patterns resembled college students, making an identification as terrorists hard
    - the network had a leadership structure but was decentralized and robust
    - a vulnerability of the network were the pilots who brought both unique skill sets and leadership to the network

Pitfalls in Network Analysis
Social Network Analysis is not always the best method to choose, so knowing when to use it and when NOT to use it is crucial. Challenges and pitfalls include:

- Reducing a social system to a network in which actors are connected in a pairwise fashion by only a single type of relationship is often an extremely crude approximation of reality.
- Incompleteness: Not all nodes may be uncovered. The incompleteness distorts results of centrality measures.
- Fuzzy boundaries: It may be difficult to decide whom to include and how far the network should reach
    - an individual with a lot of connectivity may not necessarily be relevant for the analysis (e.g., a gardener)
- Shorter paths are the most important ones to look at but not all information/influence flows along them. Thus, one should not only focus on them.
- Peripheral players might be neglected by analysts but can be important resources for the network (e.g., they could be the person who provides guidance to the group)
- Dynamic nature: Acknowledge that networks are dynamic and relationships can change
    - maintaining the mapped network can thus present a challenge
- Network analysis and especially its mathematical branch requires a sound understanding and thorough training to be effective. Poor knowledge can distort the analysis tremendously and thus do more harm than good.

Final Notes

- Engaging in Network Analysis is a major investment:
    - It requires dedicated software; software selection should be based on whether that software actually saves time with regard to answering information requirements
    - The learning curve is steep; training and a mentor are needed
    - BUT: Time spent saves time down the road
- Network Analysis informs the analysis but it is NOT immediately providing answers to the so what? and what's next?
    - Using Network Analysis allows tracing back how the analyst came to a conclusion and challenge his line of evidence
    - drawing networks can be powerful tool to communicate analyses
- Other SATs should complement network analyses:
    - Key assumptions check
    - Red hat analysis
    - Circle boarding or Starbursting:
        - In essence, Circleboarding is a brainstorming technique in which analysts aim to capture different aspects of an issue by seeking answers to Who, What, How, When, Where, Why, and So What?
        - In the context of SNA, these questions could be: Who am I looking for? What are they doing with whom? When are they having those meetings, how does it change over time?

Key Takeaways

- Use NA to connect the dots between people, groups and other entities
- Using software is advisable because it allows you to stay flexible and move things aroundCircle boarding
    - Knowing how the algorithm works is key for making valid assessments.
- Identify gaps in knowledge and try to tap connections:
    - What are collection sources and how can they tap a network to further describe the dynamics and relationships within?
- NA can be used to easily make a powerful (visual) case
    - A simple chart can be very helpful and powerful in your presentation to make your case