Notes from Session 8

Security and Defence III

There were the following comments in the plenary discussion of the third and last session on Security & Defence:

- There is no good way to validate the command structures that are suggested by various methods.
- There is always a snitch willing to validate command structure – if you know where to look.
- Sometimes if you don't have the absolute ground truth, you can keep the last bit of information out of your knowledge base as a control for comparison.
- How many levels of filters were used in the IMM method? It depends on the application. For tactical ballistic missile defence, you need special filters. Most applications require only 3 levels. There is almost no time lag.
- Normal Kalman filters were not used.
- Is there real time surveillance for aircraft? There could be a model that alerts on deviation of civilian aircraft from the filed flight plan.
- There are predictive behaviour patterns based on imagery to determine if a behaviour is "normal" or presents a possible threat.
- You deal with communications between people and based on the communications between them you presume a hierarchy of the network. There may be levels of networks that are parallel from each other such as the policy networks, the date shops, the support networks and there may be a one to one relationship between persons in these parallel networks. Does your method enable you to see that? Yes – in one of the examples we found three clusters. And we can go beyond that to find the organizers for these networks.
- Often what one wants to do is not take out nodes but take out links. This is the topic of current research.
- These algorithms are data hungry but you are restricted to using the open source data that is available for experimentation.
- How susceptible are these methodologies to countermeasures if insurgents decide to throw it off.
- Intelligence agencies cannot succeed without researchers and researchers cannot succeed without intelligence agencies – we need a network to fight a network.
- Researchers need a clue from the intelligence community that they are going down the right path or not.
- Masked data has been requested but the analysts have not followed up to make good on the agreement.
- Have you experimented with adding noise to a node instead of removing a node? We have not since there is already a lot of noise in the data. This would be an interesting experiment on the affect of information.
- There are less subversive social networks perhaps that could be useful for testing.
- Perhaps NATO could take on the responsibility of answering requests for masked data by uncleared researchers - perhaps a repository of masked data.
- Suggest a representative data set for social network testing.

- The desire to publish is part of the problem.
- If you have a good idea, you don't have to publish with the military domain data, you can convert to another domain for the purpose of the publication.
- Suggest you attend conferences as often as you can and establish contacts – see ISNA.org.
- For the disaster management application, the data dribbles in over a period of time. If that data dribbles in the form of sticky notes or white boards, how can you take that into account? We currently assume the data is entered in a database somewhere.
- There are human factors advantages to white boards and other more conventional paper-based methods.
- Automated reports would be a good feature to build in.