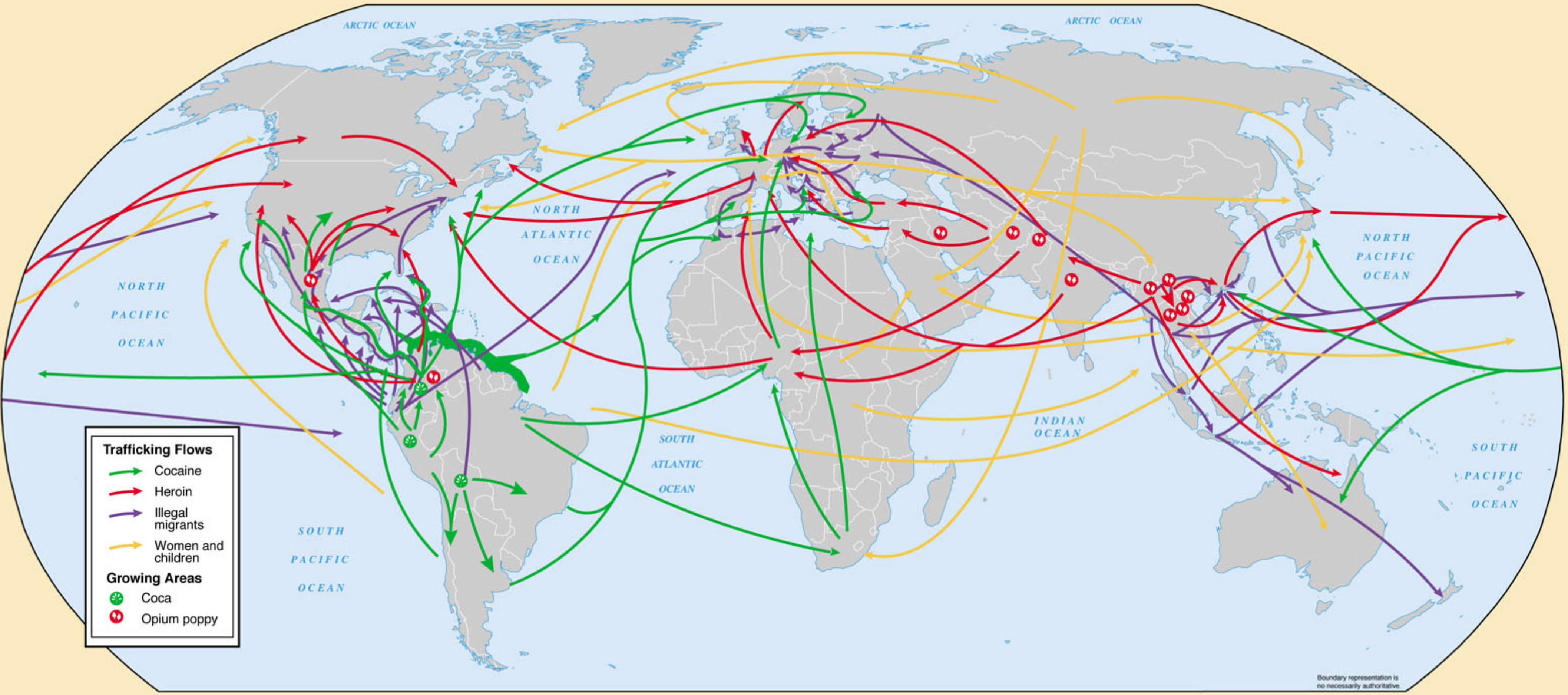
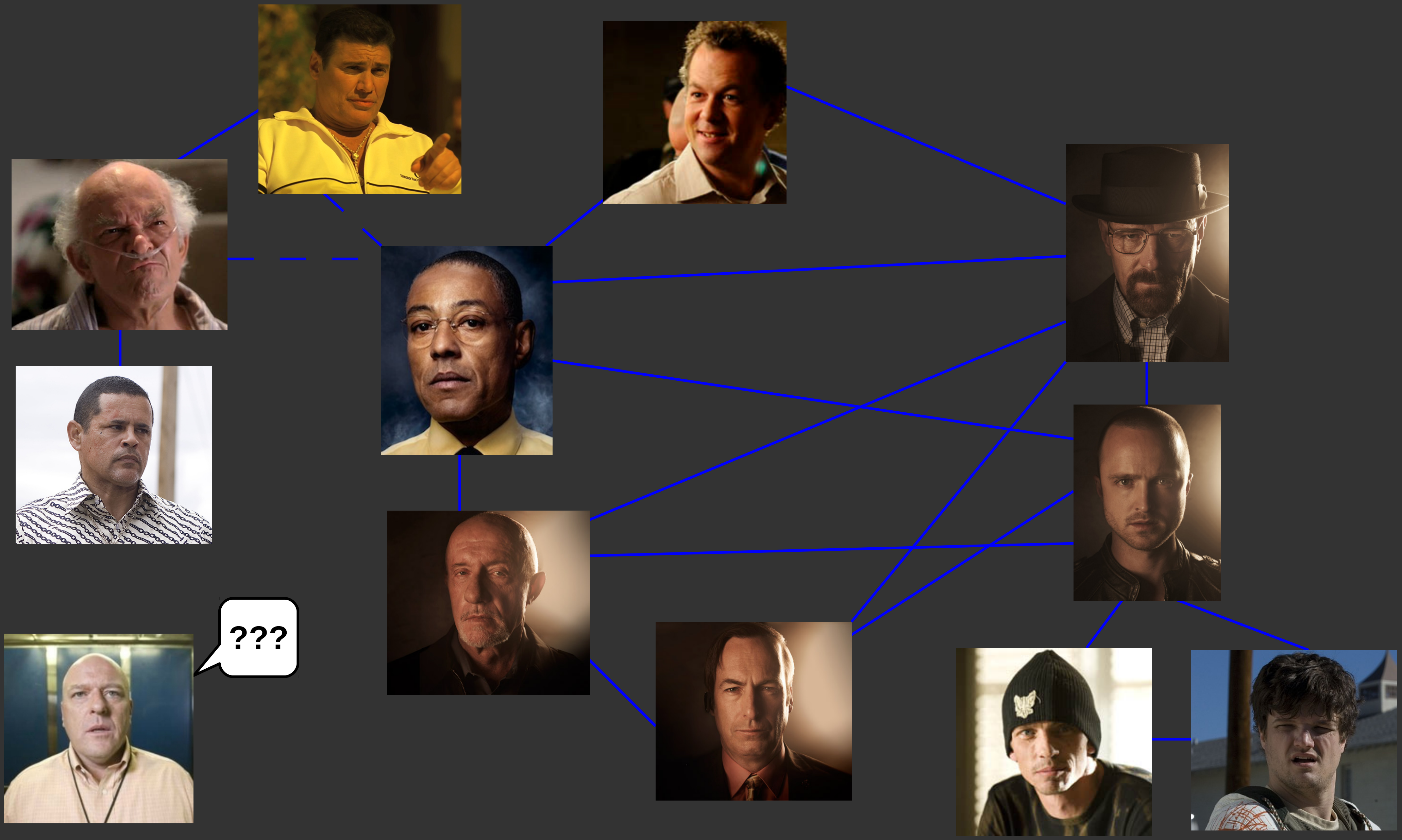


Network analysis in criminal intelligence

Alex Richert, PHYS 580, Fall 2012, PSU

The "chain of command" model of organized crime is outdated

Modern crime is complex



Many types of crime can be modeled with networks

- Financial crime (racketeering, money laundering)
- Illegal trade networks (drugs, small arms, humans)
- Cyber crime (identity theft)
- Terror networks

The 9/11 terror network

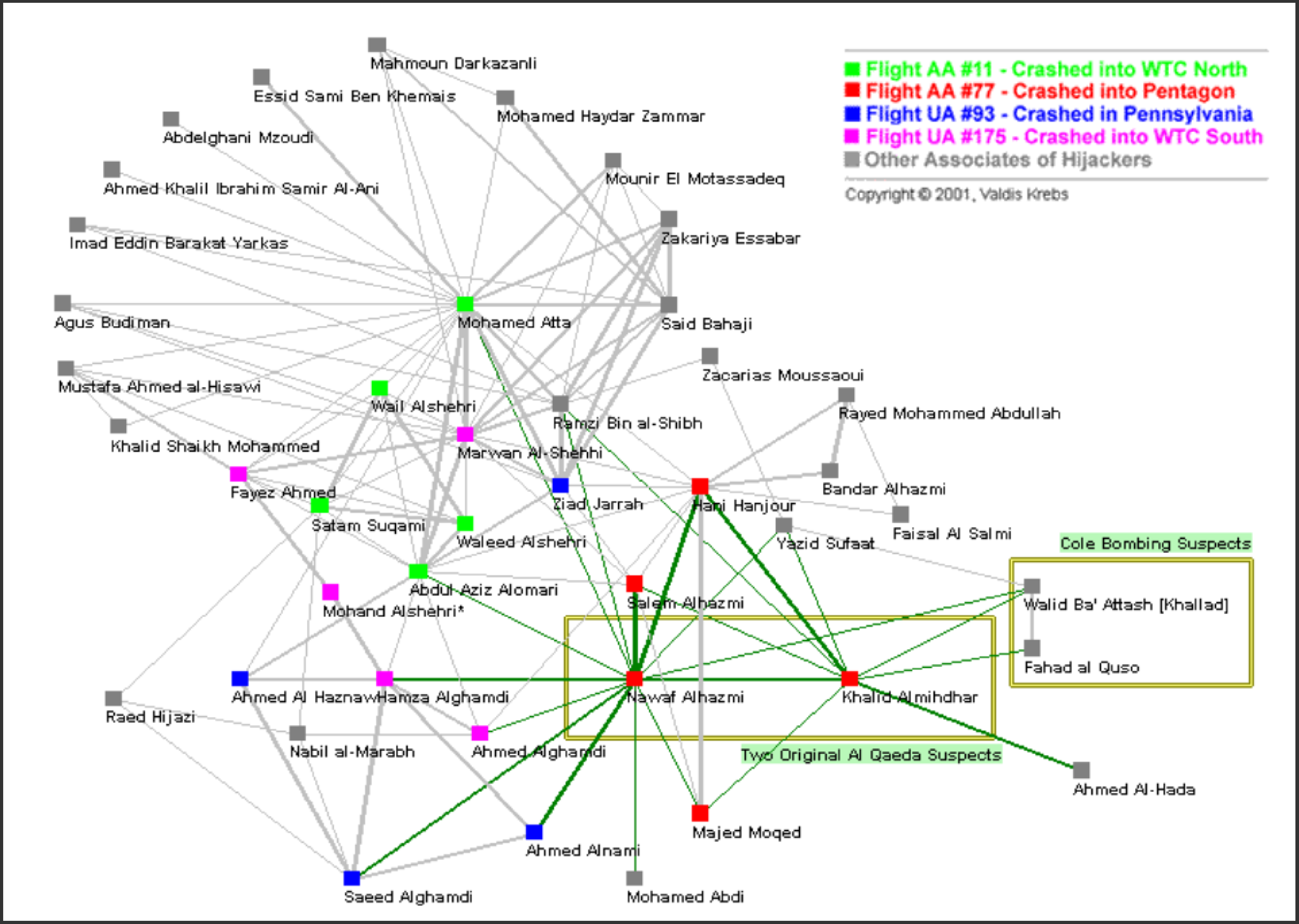


Figure by Valdis Krebs

Representation depends on type of investigation and available data

- Typical networks involve individuals (nodes) and relationships (edges) such as:
  - Trust (family, friends, work)
  - Task (phone calls, email, travel/meetings)
  - Money (bank accounts, spending patterns)
- Directed networks and weights can be important, especially for illegal trade networks
- Bipartite networks (organizations, demography, geography)

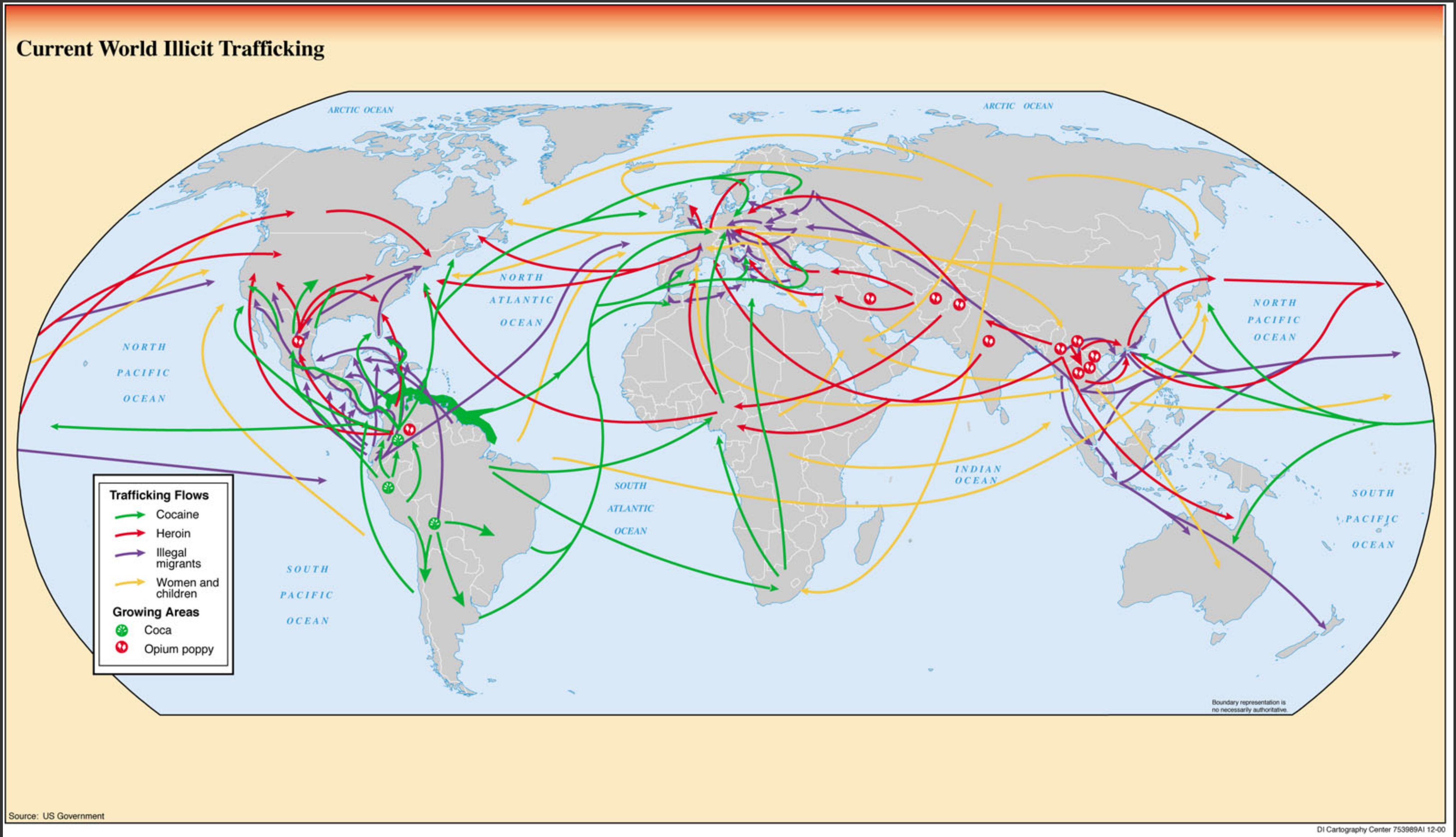


Figure from Global Trends 2015, National Intelligence Council, 2000

Analysis

- Visualization
- Template-matching
- Network measures
- Completeness/bias

Visualization: the basic application of networks

- Visualization was the first application of networks to criminal investigation
- Guides the intuitions of investigators and aids in report delivery

Template-matching helps to determine network roles

- Big Floyd (FBI) was the first use of networks for automated analysis
- Data are matched against model criminal organizations (“templates”)
- Identifies likely roles based on known relationships
- Requires robust, accurate models, which will depend on type of crime and size of network

Choice of network measure depends on type of crime and police goals

- **Size** may determine key aspects of investigation
- **Degree** (number of contacts, buyers, sellers)
- **Betweenness** (weights will give throughput)
- **Closeness** (might tell police who to question)
- **Point strength** (important for network fragmentation)

Incomplete data may lead to bias

- Statistics like node degree will depend on investigator bias and secrecy of entities
- The effect of missing data depends on:
  - Network size
  - Network type
  - Random vs. non-random
- This problem is solved through quantity and quality of information, as well as appropriate network representations

Conclusions

- Network analysis in criminal intelligence is a growing field with diverse applications
- Academic research is still limited, though applications are increasing
- Future research and applications:
  - Scaling of criminal networks
  - Time dynamics
  - Dynamics of link/node removal (network disruption)

References and further reading

- **Klerks, P. 1999, Connections, 24(3), 53**
- Krebs, V. 2002, Connections, 24(3), 43
- Mahmoud, T., & Trebesch, C. 2010, Journal of Comparative Economics, 38, 173
- Obuah, E. 2006, International Politics 43, 241
- **Sparrow, M. 1991, Social Networks, 12, 251**