Dismantling and disrupting criminal networks: A research perspective.

Dr David Bright
Dr Catherine Greenhill (Mathematics and Statistics)

Criminal Networks Research Group
www.cnrg.unsw.edu.au
Acknowledgments

Collaborators:
- Professor Alison Ritter, Drug Policy Modelling Program (UNSW)
- Professor Carlo Morselli (University of Montreal)
- Dr Caitlin Hughes, Drug Policy Modelling Program (UNSW)
- Dr Jenny Chalmers, Drug Policy Modelling Program (UNSW)
- Dr Helen Finn, School of Social Sciences (UNSW)
- Ms Natalya Levenkova, School of Mathematics and Statistics (UNSW)
- Mr Jordan Delaney, School of Social Sciences (UNSW)

Funding:
- Australian Research Council (Discovery Grant DP120101744)
- Drug Policy Modelling Program (Funded by Colonial Foundation Trust)
Overview of presentation

• Strengths and vulnerabilities in criminal networks

• Who is the key player?
  – Node attributes/roles
  – Multiple link types/resource flows

• Impact of law enforcement interventions
  – Simulation/modelling studies
Criminal Networks

• Criminal networks
  – Loose connections, dynamic
  – May include hierarchy, freelance elements

• Covert settings demand specific interactions and relational features

• Focus on security:
  – Limit physical interaction
  – Buffers between individuals
  – Decentralisation of management
Research on dismantling criminal networks

• Exploratory SNA
  – Visualisation
  – SNA metrics

• Computer simulations to test strategies
Caveats

• Data limitations

• SNA is not decision-making (Everton, 2013)
  – Knowledge of context?
  – Risks?
  – Costs?
  – Unintended consequences?
Criminal networks: strengths

• Facilitate flow of tangible/intangible commodities
• Flexible and dynamic
• Individuals can remain hidden
• Structure for resource pooling
• No central governing authority
• Networks can “learn”

(e.g., Williams, 2001; Kenney, 2007; Morselli, 2009)
Criminal networks: vulnerabilities

- Efficiency-security trade-off
- Trust is critical
  - Larger networks sacrifice security
- Highly central nodes are vulnerable
- Arrest of one individual can cascade through network
- No central control (mistakes)
- Insulation from new ideas/information
  (e.g., Williams, 2001; Kenney, 2007; Morselli, 2009; Morselli & Giguere, 2007)
Hubs as a potential weakness
Who is the key player?

(source: Albert, Jeong, & Barabasi, 2000)
Who are the “key” players?

• “There are a limited number of people who have the network of contacts within the criminal underworld, and more importantly the level of trust that enables them to bring together the suppliers, investors, contractors, customers and the situational elements to conduct a successful importation.” (Hawley, 2002; p. 46)
## Node attributes and link types

<table>
<thead>
<tr>
<th>Tangible</th>
<th>Intangible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money</td>
<td>Information</td>
</tr>
<tr>
<td>Drugs</td>
<td>Skills</td>
</tr>
<tr>
<td>Premises</td>
<td>Knowledge</td>
</tr>
<tr>
<td>Equipment</td>
<td>Labour</td>
</tr>
<tr>
<td>Precursors</td>
<td></td>
</tr>
</tbody>
</table>

Adapted from Schwartz & Rouselle (2009)
Multiple links in criminal networks

- Majority of SNA studies on criminal networks use unitary ties
- “miss[ing] critical insights into the behavior, strengths, and weaknesses of social networks by ignoring the multidimensionality of human relationships” (Hamill et al., 2008).
- Some studies have used multi-relational data
Meth manufacture-trafficking network

Adapted from Bright, Hughes & Chalmers (2012)
## Node attributes or roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers</td>
<td>Designated tasks to others, provided the funds for parts of the drug trafficking operation, or to whom other individuals reported.</td>
</tr>
<tr>
<td>Clan lab managers</td>
<td>Managed the operation of clandestine laboratory sites.</td>
</tr>
<tr>
<td>Wholesale dealers</td>
<td>Responsible for selling methamphetamine in single to multiple kilogram lots.</td>
</tr>
<tr>
<td>Resource providers</td>
<td>Sourced chemicals and equipment required for the manufacture of the drug.</td>
</tr>
<tr>
<td>Specialists</td>
<td>Possessed specialist knowledge and skill in the manufacture of methamphetamine.</td>
</tr>
<tr>
<td>Workers/labourers</td>
<td>Paid a wage to complete tasks or follow orders.</td>
</tr>
<tr>
<td>Corrupt officials</td>
<td>Occupied government positions and received bribes to behave in corrupt ways.</td>
</tr>
</tbody>
</table>

Adapted from Bright, Hughes & Chalmers (2012)
So which nodes are “key” to the network?

Adapted from Bright, Hughes & Chalmers (2012)
Study: Law enforcement simulations
(Bright, Greenhill, & Levenkova, 2013)

Our aim: to simulate a range of law enforcement strategies for intervention, taking into account both centrality and role of nodes.

Computers work with numbers: the first task was to assign a number or weight to each node, based on their role in the network.
Quantifying importance: weights

<table>
<thead>
<tr>
<th>Role</th>
<th>Nodes with that role</th>
<th>Weight of each of these nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager/Assistant Manager</td>
<td>K18, K28</td>
<td>1/2</td>
</tr>
<tr>
<td>Possession of specialist skills</td>
<td>K10, K36</td>
<td>1/2</td>
</tr>
<tr>
<td>Clan lab “branch manager”</td>
<td>K12, K24, K31</td>
<td>1/2</td>
</tr>
<tr>
<td>Corrupt official</td>
<td>K33, K34, K35</td>
<td>1/3</td>
</tr>
<tr>
<td>Wholesale dealer</td>
<td>K1, K13, K15, K23, K26, K27, K32</td>
<td>1/7</td>
</tr>
<tr>
<td>Resource provider</td>
<td>K5, K6, K7, K8, K9, K11, K14, K22</td>
<td>1/8</td>
</tr>
<tr>
<td>Worker/”labourer”</td>
<td>K2, K3, K4, K16, K17, K20, K21, K25, K29, K30</td>
<td>1/10</td>
</tr>
<tr>
<td>Unknown role</td>
<td>K19</td>
<td>0</td>
</tr>
</tbody>
</table>
Simulating an intervention:
Here is an example of a network with node weights. Now we want to choose a node to delete (remove).
Four strategies for simulations

We considered four strategies for law enforcement “interventions”:

• Target most connected nodes (high degree centrality)
• Target nodes which play most important roles
• Target by a combination of degree centrality and role
• Random selection

If two or more nodes with the same score, choose randomly between them.
Which node to target?

• the red node, if using only degree centrality;
• the green node, if using only weight;
• If centrality and weight contribute equally? Then the green node.
• If centrality counts twice as much as weight? Then the red node!
Our simulations and outcome measures

At each time step:
- choose a node (according to some fixed strategy) and delete it.
- measure the extent of disruption to the network.

But how can the “extent of disruption” be quantified?
- Number of nodes in the largest remaining connected component
- Largest connected component + weight of “most important” connected component
Example, continued:

After one deletion we have two connected components.

- The **red component** is the largest, with size 5;
- The **green component** has the most total weight, namely $8 + 2 = 10$.

Adding these two measures gives a third measure, which we called the disruption function.
Quantifying “success”

For each of the four strategies, we performed 100 runs of the simulation. This gave averages, over the 100 runs, for our two outcome measures at each time step.

We plotted each of these outcome measures (size of largest connected component, and maximum weight over all connected components) on a graph to allow us to compare the four simulations.

Which strategy was the most effective at dismantling our initial network?
The four simulations- size of the largest connected component (Bright, Greenhill, & Levenkova, 2013)
The four simulations - value of “disruption measure” (Bright, Greenhill, & Levenkova, 2013)
What works?

Manager/Assistant manager
Clan lab “branch manager”
Resource provider
Possession of specialist skills
Worker/labourer
Corrupt officials
Wholesale dealer
Unknown
Dismantle/Disrupt: What works?

• Relatively effective:
  – Targeting nodes based on
    • degree centrality
    • degree + role

• Relatively ineffective:
  – Targeting nodes based on role only

• Limitations
  – Targeting “key player” is overly simplistic; no network adaptation/change
  – Roles (individuals can have more than one attribute); links (more than one type of link);
Illicit drug trafficking: The structure of illicit networks and implications for resilience and vulnerability (ARC Discovery Project)

- Structure of drug trafficking network
  - Node attributes
  - Link types

- Design and evaluate methods for:
  - disruption
  - dismantling
## Node attributes and link types

<table>
<thead>
<tr>
<th>Tangible</th>
<th>Intangible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money</td>
<td>Information</td>
</tr>
<tr>
<td>Drugs</td>
<td>Skills</td>
</tr>
<tr>
<td>Premises</td>
<td>Knowledge</td>
</tr>
<tr>
<td>Equipment</td>
<td>Labour</td>
</tr>
<tr>
<td>Precursors</td>
<td></td>
</tr>
</tbody>
</table>

Adapted from Schwartz & Rouselle (2009)
Data sources and method

• **Data:**
  – Files from ODPP

• **Method:**
  – Part 1
    • Extract relational data, attribute data, link data
    • Construct network map
    • SNA metrics (e.g., centrality measures)
  – Part 2
    • Design and test law enforcement “interventions”
Network map
Money network
Drug network
Law enforcement simulation example

- Law enforcement intervention
  - aim: centralise the network

  - Concentrate efforts
  - Nodes easier to target
  - Key nodes more visible
  - Less adaptation/flexibility
  - Reduce competition
  - Increase price