Decision Support for Policing Violent Crime

Jim Q. Smith & Aditi Shenvi (with Rob Procter, Theo Damoulas, Mark Briers)

Uni. of Warwick & Alan Turing Institute

December 2018

What we are doing

- Building decision support systems designed to frustrate & pursue people radicalised into planning acts of extreme violence.
- Such data centric systems challenging! Vast jumble of information is available, but biased, noisy, patchy & streaming in real time.
- Includes data from sources such as social media and CCTV images, + huge data about those under surveillance.

Question - How do authorities allocate resources to this huge dynamic system in a most effective way engaging the users & supports their decisions?
Answer Use a Bayesian Decision Analysis!

What a Bayesian Decision Analysis does

- A BDA systematically **filters data streams in an intelligent & user led way**.
- Bayes methods **unique** in their maturity & scope.
- **Uncertainty** acknowledged & embedded in both expert judgements & accommodated data.
- In context of **criminal investigations** this facility is **essential** – neither intent of a suspect nor its expression certain.
- Prob. dists. derived from this analysis used to provide **risk scores** in light of uncertainty: policy options given subjective expected utility scores.

Essential element Must support users to critique, adapt & overrides it suggestions - to converse and genuinely support investigative strategies.

What we do

- Natural Language Description $\rightarrow$ Formal Defensible description $\rightarrow$ hypotheses scored by data.
- Criminological hypotheses $\rightarrow$ Probability Models$\rightarrow$ Location, Nature, Extent of Threat.
- Built round expressing individual **progression** (at idiosyncratic rates) into presenting threat to general public.
- **Graphs** used to translate profound domain insights into prob. models (some snap shots given here).
- Build on recent advances in analogous examples within forensic science & public health.

Our Framework

- Models break down description of violent criminal processes into **3 levels**.
- Recomposed to provide a **full picture of dynamically changing threat landscape** – single time varying, probability model of suspects + threat population.
- Model **draws together disparate data** into threat assessments of various suspects.

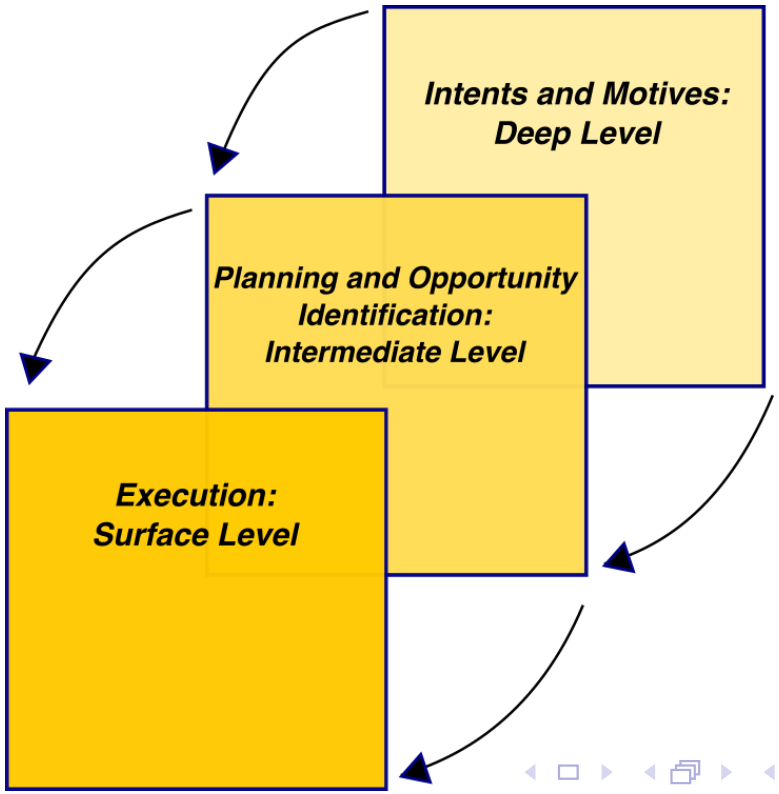

Figure: The three layer threat model.

The first of our three Levels

Deepest hidden level: customised family called reduced dynamic chain event graph (RDCEG) (see Smith & Shenvi,18).

- Graph translate expert's natural language hypotheses radicalisation processes into families of prob. models.

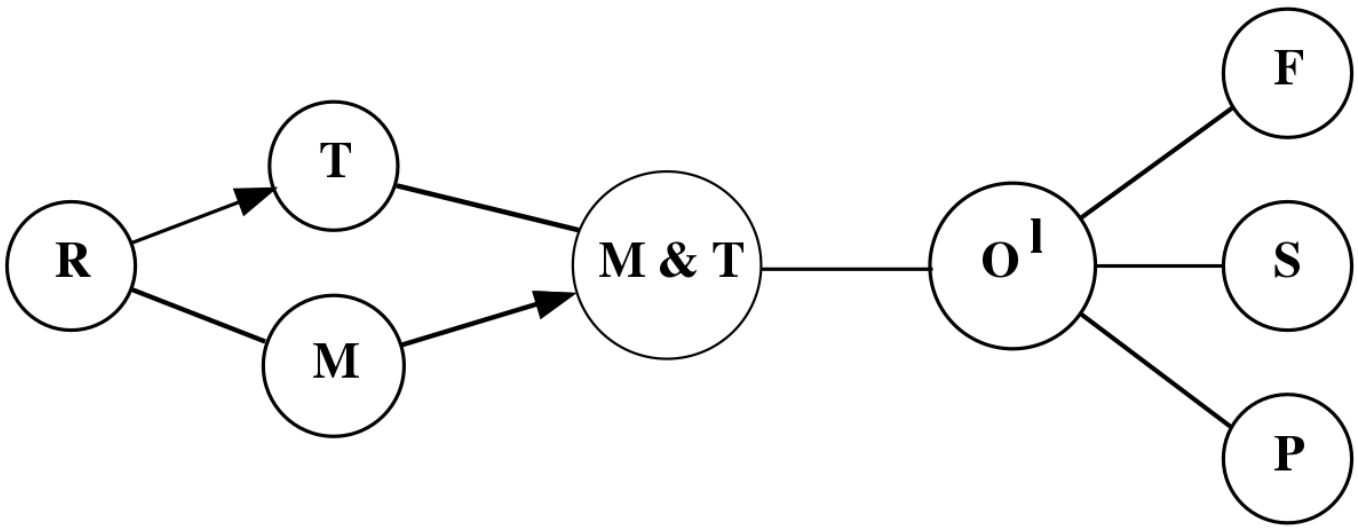

Figure: A person in position R is radicalised, M is motivated to attack, T is trained to attack, O^l is acting as a loner. Finally S, P, F denote the assault incident of the given type is a success, partial success or a failure respectively.

Other two levels

Two other levels of expert information
Intermediate hidden level: Expert judgements about the **tasks** engaged in by suspects at a particular stage of preparing a violent attack:
Final surface layer: – usually only one directly (partially) observable – describes **what people might actually do** to perform such tasks. This linking data streams to tasks and hence to states.

Fact

All levels of our model + software built from expert structural judgements & continual user revision populating it with new current external info.

Radicalisation and process: defining the first graph

- Motive, Means, Opportunity - Intent, Capability, Preparation

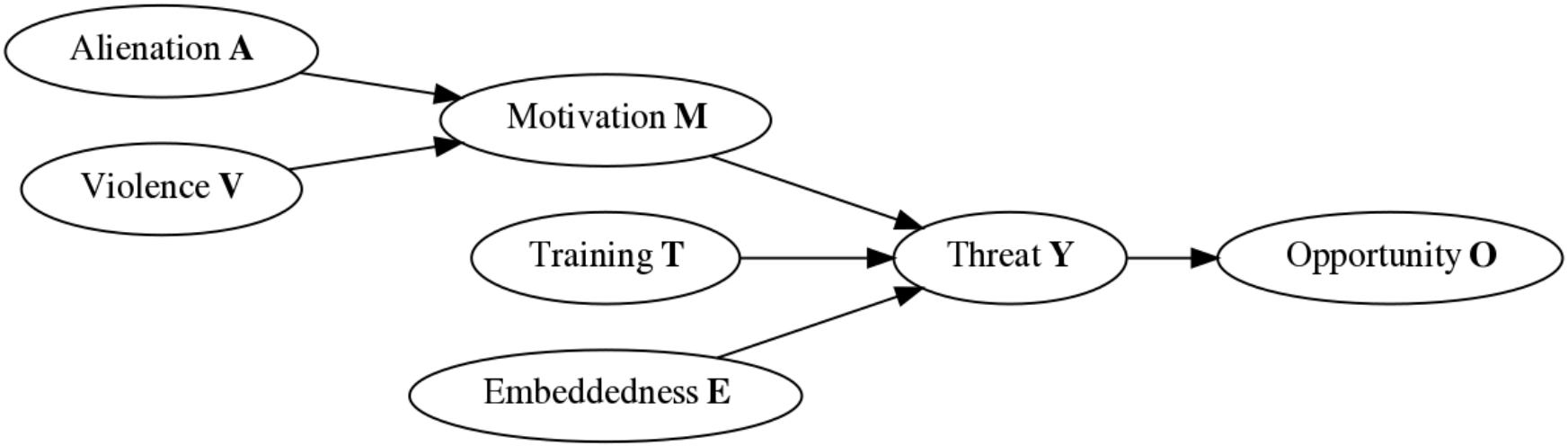

Figure: Computation graph summarising the radicalisation process based on the key features of mean, motive and opportunity.

Alienation Questionnaire

- $\mathbf{a_1} - \mathbf{a_3}$: Benign states with potentially some dissatisfaction with life.
- $\mathbf{a_4}$: Society must change; it can't support right thinking people like me. I need to align myself to a group of other outsiders.
- $\mathbf{a_5}$: Revolutionary change is needed to transform mainstream society so that people like me can participate.
- $\mathbf{a_6}$: Mainstream society is my enemy; its processes and people need to be actively undermined.
- $\mathbf{a_7}$: Any acts - criminal or not - that attack and undermine the current order are fully justified; I wholeheartedly support such acts.
- $\mathbf{a_8}$: Those who do not align with my perspectives are to be despised. My personal vocation is to align everyone to my world view using all means possible.

Violence Questionnaire

- $\mathbf{v_1}$: Would never knowingly physically harm someone or support criminal acts.
- $\mathbf{v_2}$: Could envisage circumstances when I support someone assaulting someone else but I could never perpetrate this act myself.
- $\mathbf{v_3}$: In extreme circumstances I might be prepared to assault someone myself.
- $\mathbf{v_4}$: Whenever necessary I will reluctantly personally assault another person.
- $\mathbf{v_5}$: I am quite happy to physically assault someone if necessary.
- $\mathbf{v_6}$: I am eager to assault someone if given the opportunity.

Matrix to motivation

Alienation\Violence	v_1	v_2	v_3	v_4	v_5	v_6
a_1	m_0	m_0	m_0	m_0	m_0	m_0
a_2	m_0	m_0	m_1	m_1	m_1	m_4
a_3	m_0	m_0	m_1	m_1	m_1	m_4
a_4	m_0	m_0	m_1	m_1	m_2	m_4
a_5	m_0	m_0	m_2	m_2	m_2	m_4
a_6	m_0	m_0	m_2	m_2	m_2	m_4
a_7	m_0	m_0	m_2	m_3	m_4	m_4
a_8	m_0	m_0	m_4	m_4	m_4	m_4

Coarse categories of violent motivation listed in escalating order
m_0 - **immune**; m_1 - **benign**; m_2 - **open to adopting**
m_3 - **aligned**; m_4 - **enactor**.

Training Questionnaire

- Untrained in playing a role r in a criminal assault of type g.
- Partially trained to enact r in a criminal assault of type g.
- Fully trained to enact r in a criminal assault of type g.

Embeddedness Questionnaire

- Not meeting every two weeks with like minded criminals and embedded in contacts with immune people.
- Meeting every two weeks remotely, for example electronically with like minded criminals and embedded in contacts with immune people.
- Meeting every two weeks electronically and physically with like minded criminals while in full contact with immune people.
- Meeting every two weeks electronically and physically with like minded criminals and contact with immune people reduced by at least 50% from two years ago.
- Meeting regularly electronically and physically with like minded criminals and contact with immune people reduced to less than 10% from two years ago.

The lone attacker

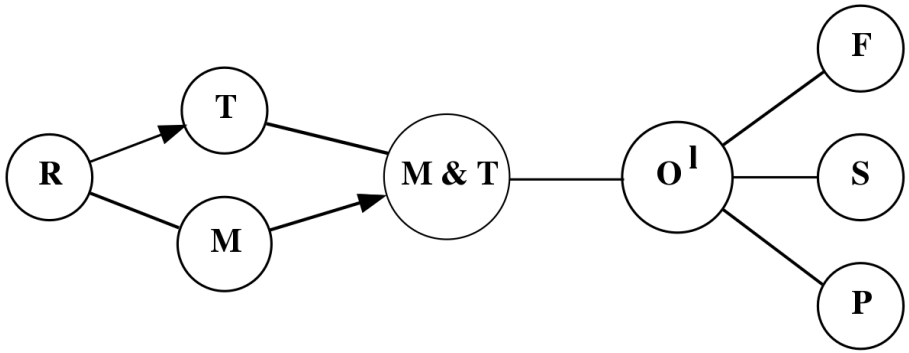

Figure: A person in R is radicalised, M is personally motivated to attack, T is personally trained to attack and O^I is acting as a loner. Finally S, P, F denote the assault incident is a success, partial success or a failure respectively. State I denotes the immune state.

	R	M	T	M&T	O^I	S	P	F	I
R	$*$	$*$	$*$	0	0	0	0	0	$\star$
M	$*$	$*$	0	$*$	0	0	0	0	$\star$
T	0	0	$*$	$*$	0	0	0	0	$\star$
M&T	0	0	$*$	$*$	$*$	0	0	0	$\star$
O^I	0	0	0	$*$	$*$	$*$	$*$	$*$	$\star$
S	0	0	0	0	$*$	0	0	0	$\star$
P	0	0	0	0	$*$	0	0	0	$\star$
F	0	0	0	0	$*$	0	0	0	$\star$
I	0	0	0	0	0	0	0	0	$\star$

Vehicle attacker fleshing out

- **Deep level** Radicalised man is currently intent on using a lorry as a weapon against the general public.
- **Intermediate level**. **M&T state** $\rightarrow$ **O Tasks** - Choose where to attack, when & how to get there, get lorry to make attack.
- **Surface level** : **activities on CCTV** visit target venue, travel to check timings, density of victims & defences. **electronic** Inspect Google maps of attack area and route there phone calls to collaborators for advice **intelligence** hire or steal lorry just before the attack.

Fact

Subsets of potentially observable actions provide indirect information about imminence of threat a suspect poses at the deep level.

Key challenges we currently face

- **Dynamics of the surface layer**: Signals depend heavily on who is observed – their preferred modus operandi + data available at any time - in continual flux!
- **Disguise**: How to customise extracted signals to be robust against decoy behaviour.
- **Embedding external information**: DSS must facilitate the manual input of new external info. to calibrate to ongoing investigation.
- **Provision of fast transparent communication**: user can confidently modify inputs in real time.

Success just depend whether tool works. Needs to be adopted!
Hardest job for geeks like us to make our methods transparent to the less geeky users.
Time & patience from both sides needed! But we're getting there.

Watch this space!!!

Selected Publications by authors

Collazo, R.A. & Smith, J.Q.(2018) "An N Time-Slice Dynamic Chain Event Graph" (submitted)
Smith J.Q. & Shenvi, A. (2018) "Assault Crime Dynamic Chain Event Graphs" Math Archive
Collazo, R.A., Gorgen,C. & Smith, J.Q.(2018) "Chain Event Graphs" Chapman and Hall
Collazo, R.A. and Smith, J.Q.(2017) "The Dynamic Chain Event Graph" Proceedings of ISI Marrakech,
Thwaites P.A. & Smith J.Q.(2017) "A Graphical method for simplifying Bayesian Games" Reliability Enginereering &Safety Systems(online:12-MAY-2017 DOI: 10.1016/j.ress.2017.05.012
Collazo, R.A. & Smith, J.Q.(2016) "A new family of Non-local Priors for Chain Event Graph model selection" Bayesian Analysis 11, no 4, 1165 - 1201
Cowell, R.G. & Smith, J.Q. (2014) "Causal discovery through MAP selection of stratified chain event graphs" E. J of Statistics vol.8, 965 - 997