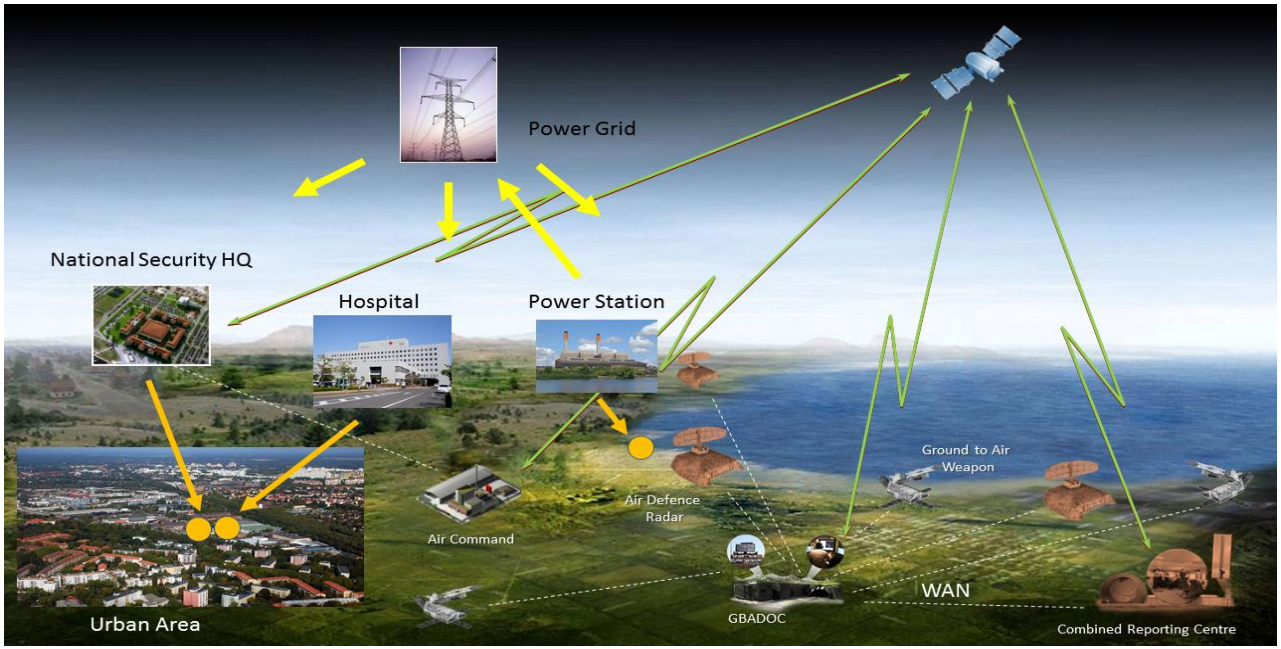
A Novel Hybrid Modelling Approach

A Novel Hybrid Modelling Approach



Bharat Patel, Dstl

Andy Kinder, ATEQ Consulting

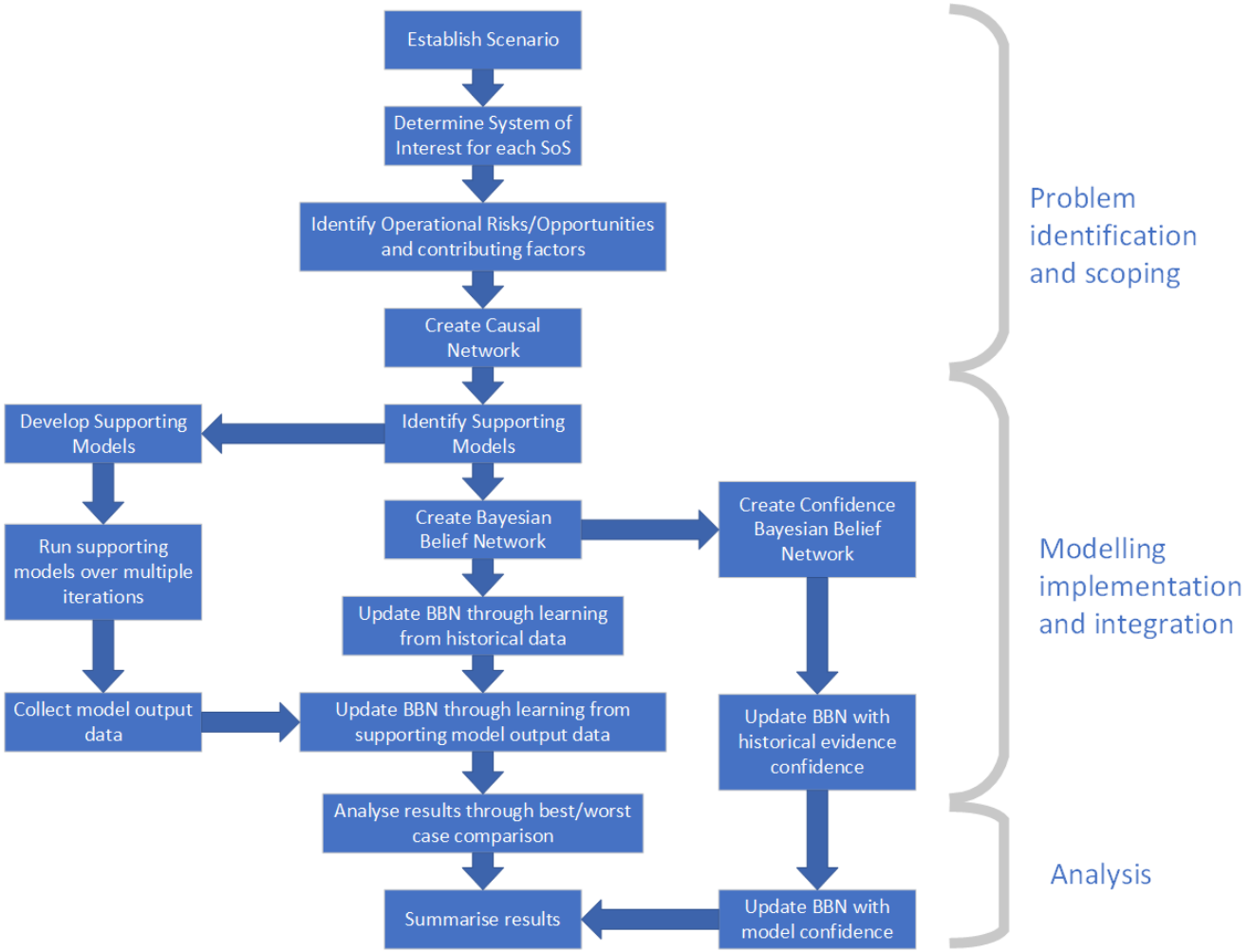
Motivation and Content

- Motivation
  - Modelling activities tend to focus upon traditional, physical effects
  - Non-traditional effects, including human and cyber, are now integral to many hybrid scenarios and therefore require modelling
- Hybrid Modelling Approach
- Case Study
- Future Exploitation
- Conclusions

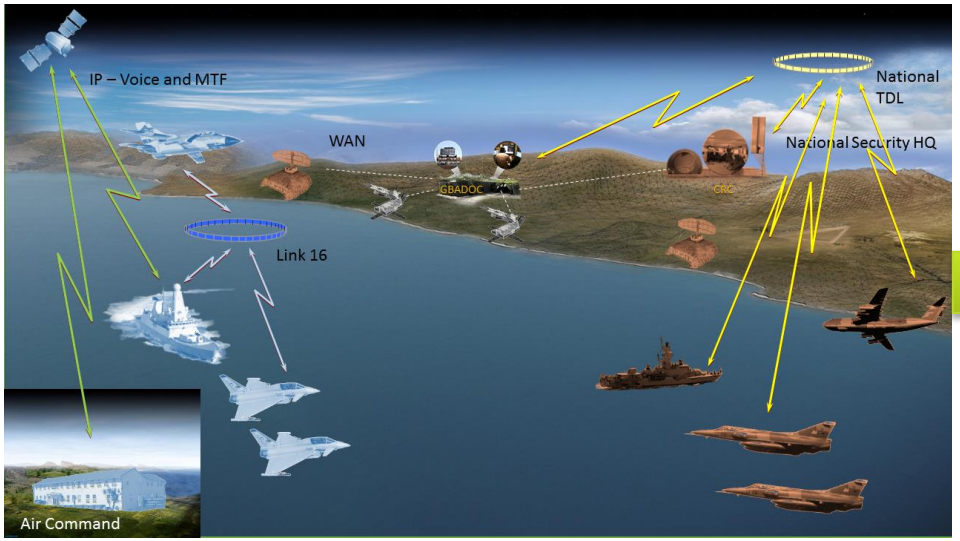
Hybrid Modelling Approach

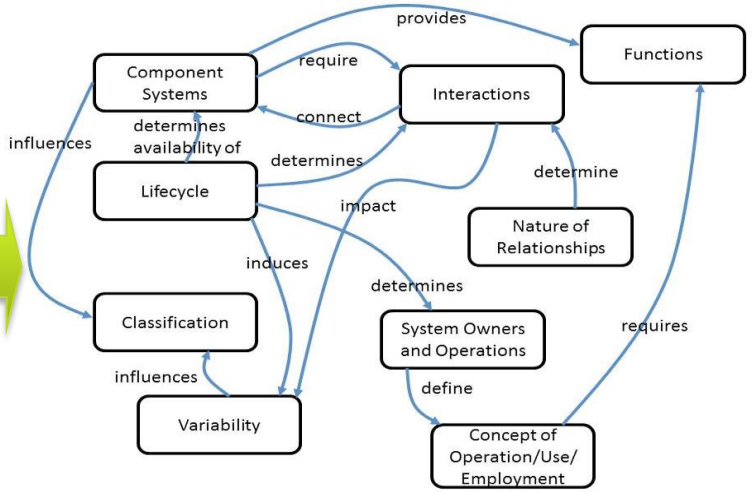
- A hybrid modelling approach has been developed from the perspective of the holistic nature of System of Systems operational risk and opportunity
  - Allows the interaction of behaviours influencing operational risk/opportunity to be modelled and enables the integration of heterogeneous modelling techniques
  - Ensures the use of modelling methods appropriate to individual behavioural characteristics, as opposed to a ‘one size fits all’ approach
  - This is particularly applicable to “Hybrid” scenario

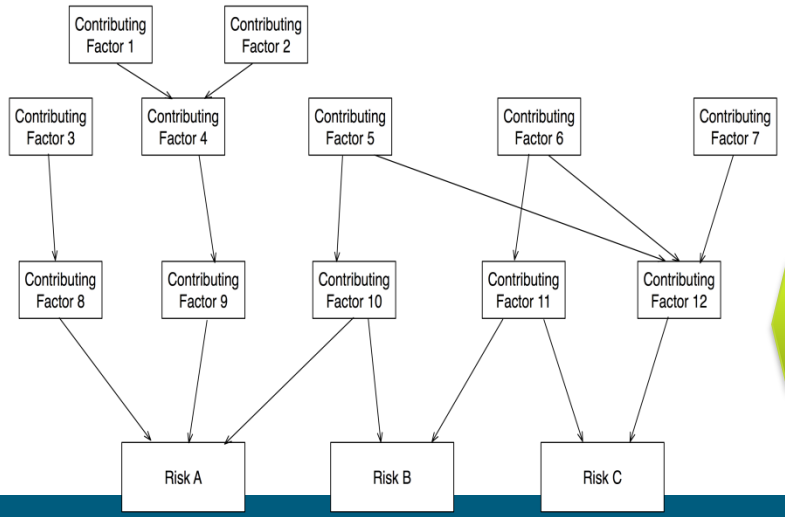
Hybrid Modelling Approach



Problem identification and scoping







SoS Dimension	Hazard	Control	Opportunity
Component Systems	Emergent behaviour inhibits purpose	System immaturity System unavailability	Emergent behaviour enhances purpose
Interactions	N/A	Misclassification	N/A
Lifecycle	Poor interoperability Bandwidth insufficient	Poor interoperability interrupts command and control	Bandwidth can support additional interaction medium
Variability	Failure dependent on a single node	Hierarchical command structure inhibits agility	Agility increased
Classification	Immaturity of component systems	Lack of coordination	Lifecycles of component systems align
Functions	SoS instability	Instability inhibits control	High agility
Systems Owners and Operations	Functions not available	Ownership of function not defined	Additional functionality exists
Concept of Operation	Lack of co-operation	Lack of management authority	High level of co-operation
Nature of Relationships	Concept of operation not supported	No clear concept of operation	Adaptable for changing concept of operation

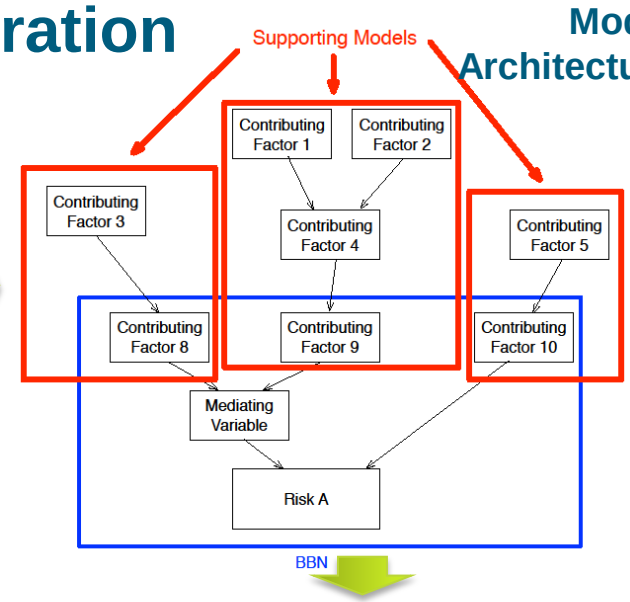
Modelling Implementation and Integration

Model Components	Dynamic	Stochastic	Uncertainty	Component Systems	Interactions	Lifecycle	Variability	Classification	Functions	Systems Owners and Operations	Concept of Operation / Employment	Relationships	Ease of creation	Verifiable
Common Digital Comms	No	Yes	No	No	No	Operational	Yes	Acknowledged	No	No	Yes			
Common Datum	No	Yes	No	No	No	Operational	Yes	Acknowledged	No	No	Yes			
Nationalities	No	Yes	No	No	No	Operational	Yes	Acknowledged	No	Yes	Yes			
Common Language	No	Yes	No	No	No	Operational	Yes	Acknowledged	No	Yes	Yes			
Common Voice Comms	No	No	No	No	No	Operational	Yes	Acknowledged	No	No	Yes			

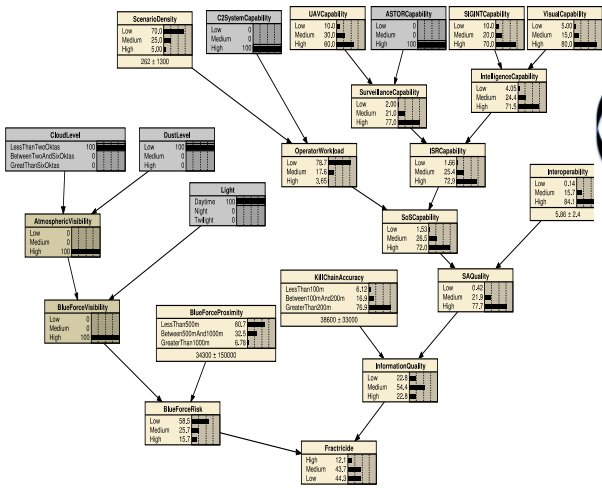
Modelling and Simulation (M&S) Techniques

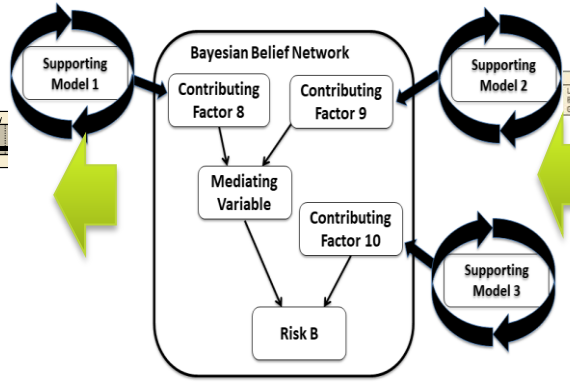
	0	4	0	0	0	0	5		0	2	5	0		
DES/DEVS	HIGH	HIGH	LOW	HIGH	HIGH	LOW	LOW	LOW	HIGH	LOW	LOW	HIGH	LOW	HIGH	1
Petri Nets	HIGH	HIGH	LOW	HIGH	HIGH	LOW	LOW	LOW	LOW	LOW	LOW	HIGH	LOW	HIGH	1
ABMS	HIGH	HIGH	LOW	HIGH	HIGH	LOW	LOW	LOW	HIGH	LOW	LOW	LOW	LOW	HIGH	1
System Dynamics	HIGH	HIGH	LOW	LOW	LOW	HIGH	HIGH	HIGH	LOW	HIGH	HIGH	LOW	LOW	HIGH	4
Surrogate Models	HIGH	HIGH	LOW	HIGH	LOW	HIGH	LOW	LOW	LOW	LOW	LOW	LOW	LOW	HIGH	1
ANN	HIGH	LOW	LOW	LOW	LOW	HIGH	HIGH	HIGH	HIGH	LOW	LOW	LOW	HIGH	HIGH	1
BNN	LOW	LOW	HIGH	LOW	LOW	HIGH	HIGH	HIGH	LOW	HIGH	HIGH	LOW	HIGH	HIGH	3
Markov Models	LOW	LOW	HIGH	LOW	LOW	HIGH	HIGH	HIGH	LOW	HIGH	HIGH	LOW	HIGH	HIGH	3
Game Theory	LOW	LOW	HIGH	LOW	LOW	HIGH	HIGH	HIGH	LOW	HIGH	HIGH	LOW	LOW	LOW	3
Decision Trees	LOW	HIGH	LOW	LOW	LOW	HIGH	HIGH	HIGH	LOW	LOW	LOW	LOW	HIGH	HIGH	2
Network Models	LOW	LOW	LOW	LOW	LOW	HIGH	LOW	HIGH	LOW	LOW	LOW	HIGH	HIGH	HIGH	0
EAF	LOW	LOW	LOW	HIGH	HIGH	HIGH	LOW	HIGH	LOW	HIGH	HIGH	HIGH	HIGH	LOW	2
Modelling Languages	LOW	LOW	LOW	HIGH	HIGH	LOW	LOW	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	LOW	2
Monte Carlo	HIGH	HIGH	LOW	LOW	LOW	HIGH	HIGH	HIGH	LOW	LOW	LOW	LOW	HIGH	HIGH	2

Model Architecture

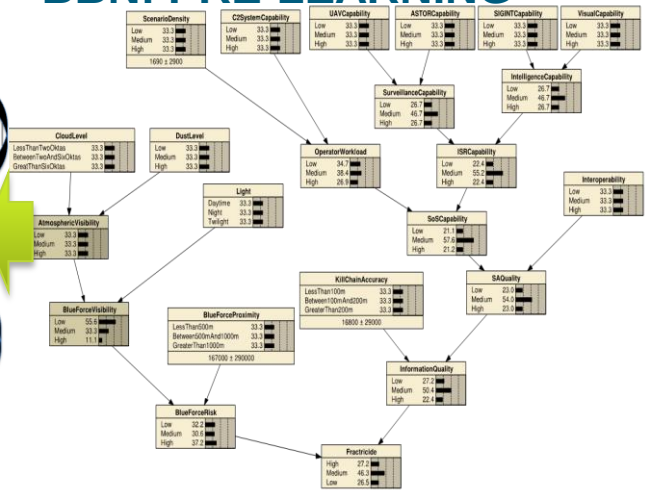


BBN: POST-LEARNING

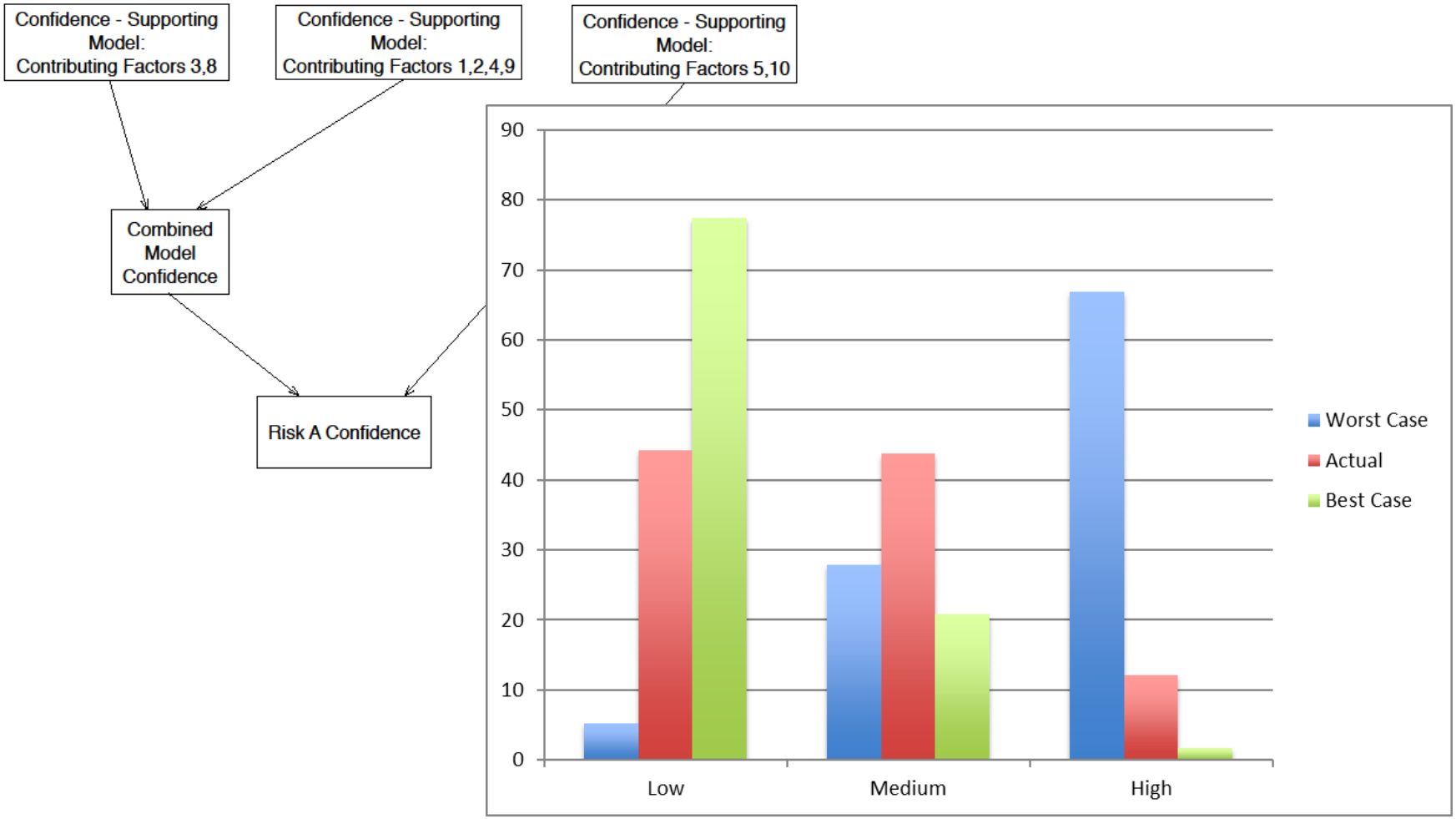




BBN: PRE-LEARNING



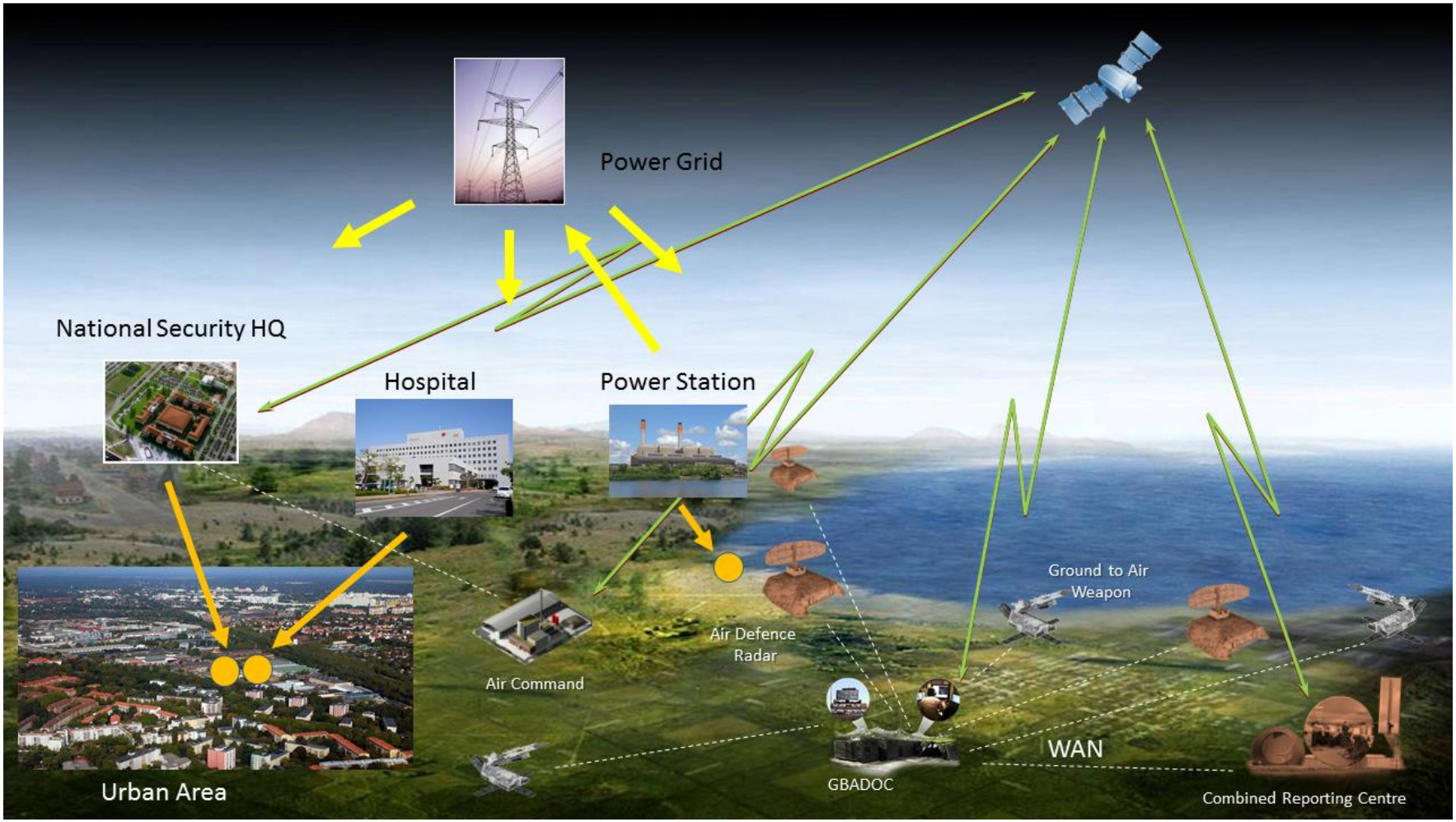
Analysis



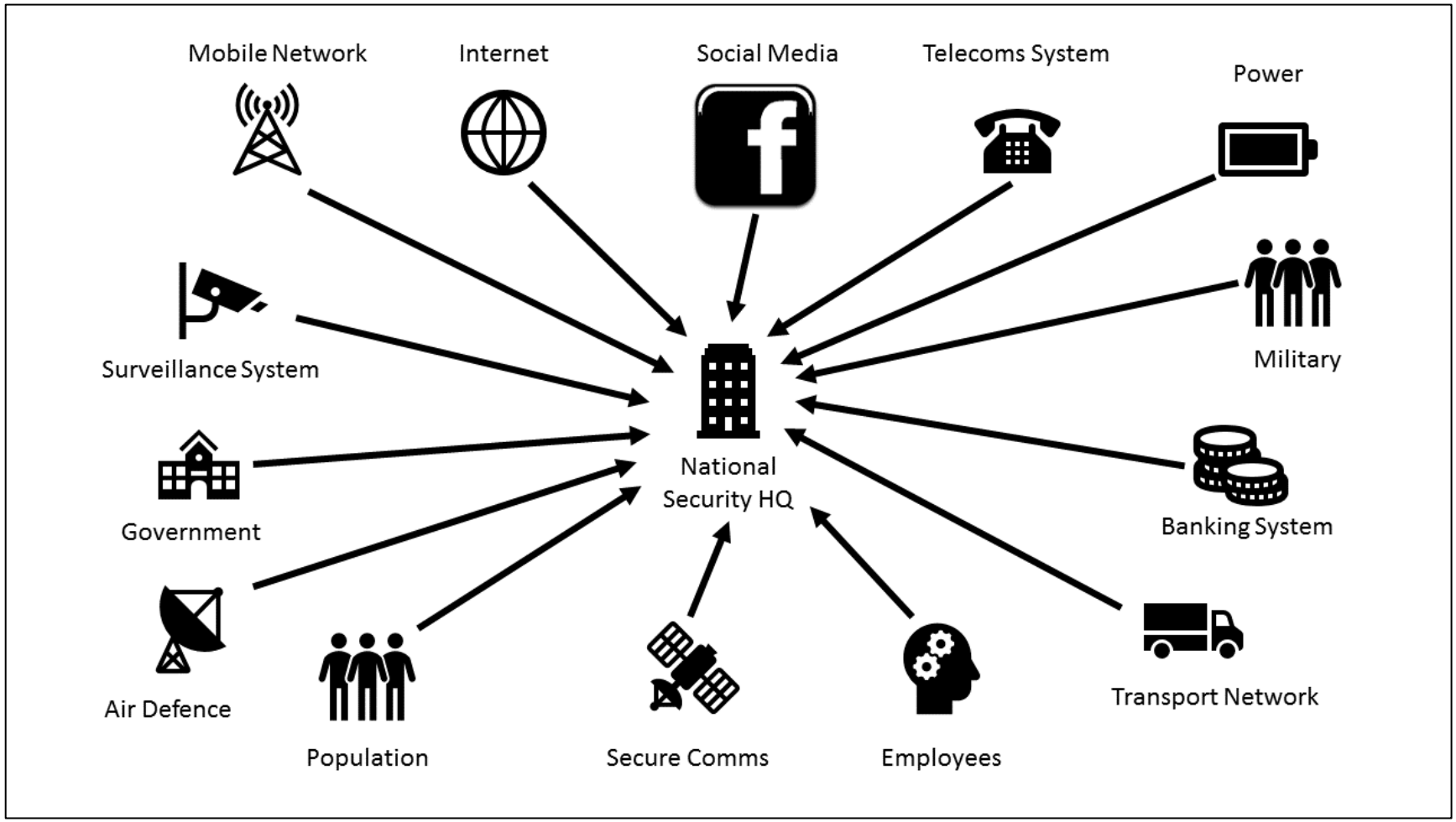
Case Study – Hybrid Scenario

- An illustrative hybrid scenario
  - Mission Purpose:
    - To counter National Security HQ operations, which have been identified as a source of several major cyber-attacks by Nation B against Nation A.
  - Context:
    - The scenario is defined from the viewpoint of a “blue” force (Nation A) intending to counter the capability of a National Security HQ (Nation B), defended by “red” forces.
  - Description
    - National Security HQ is located within a heavily populated urban area
    - Power is distributed through a national grid
    - Nation B provides comprehensive broadband and mobile networks
    - Its citizens have unrestricted, but monitored, access to the world wide web, and hence to social media
    - The national infrastructure is highly networked and therefore reliant on access to the internet
    - Nation B is not considered to be fully democratic, with a longstanding but unpopular government
    - Nation B’s air defence system comprises a series of radar and ground-to-air missile sites co-ordinated

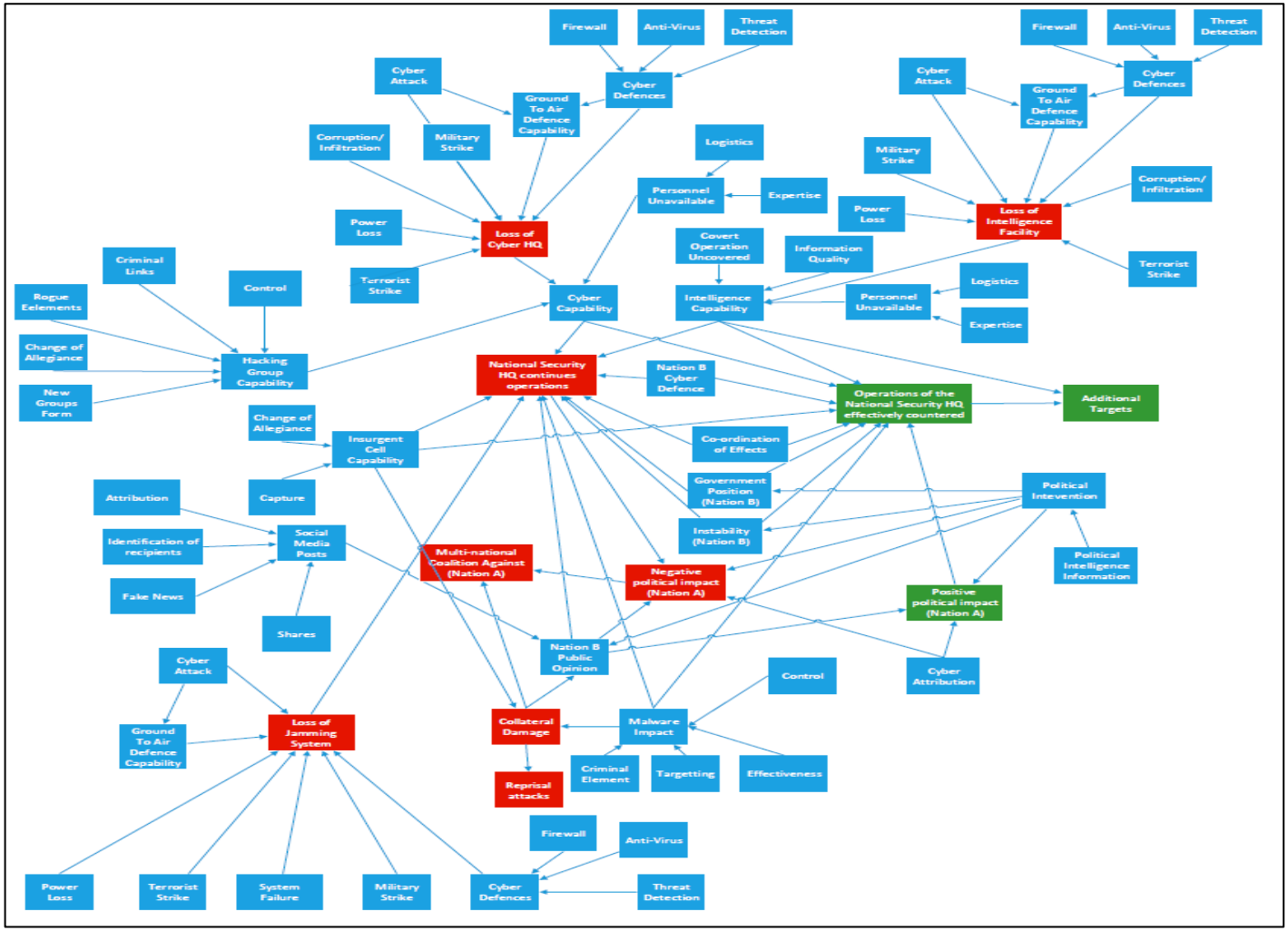
Hybrid Scenario – Nation B



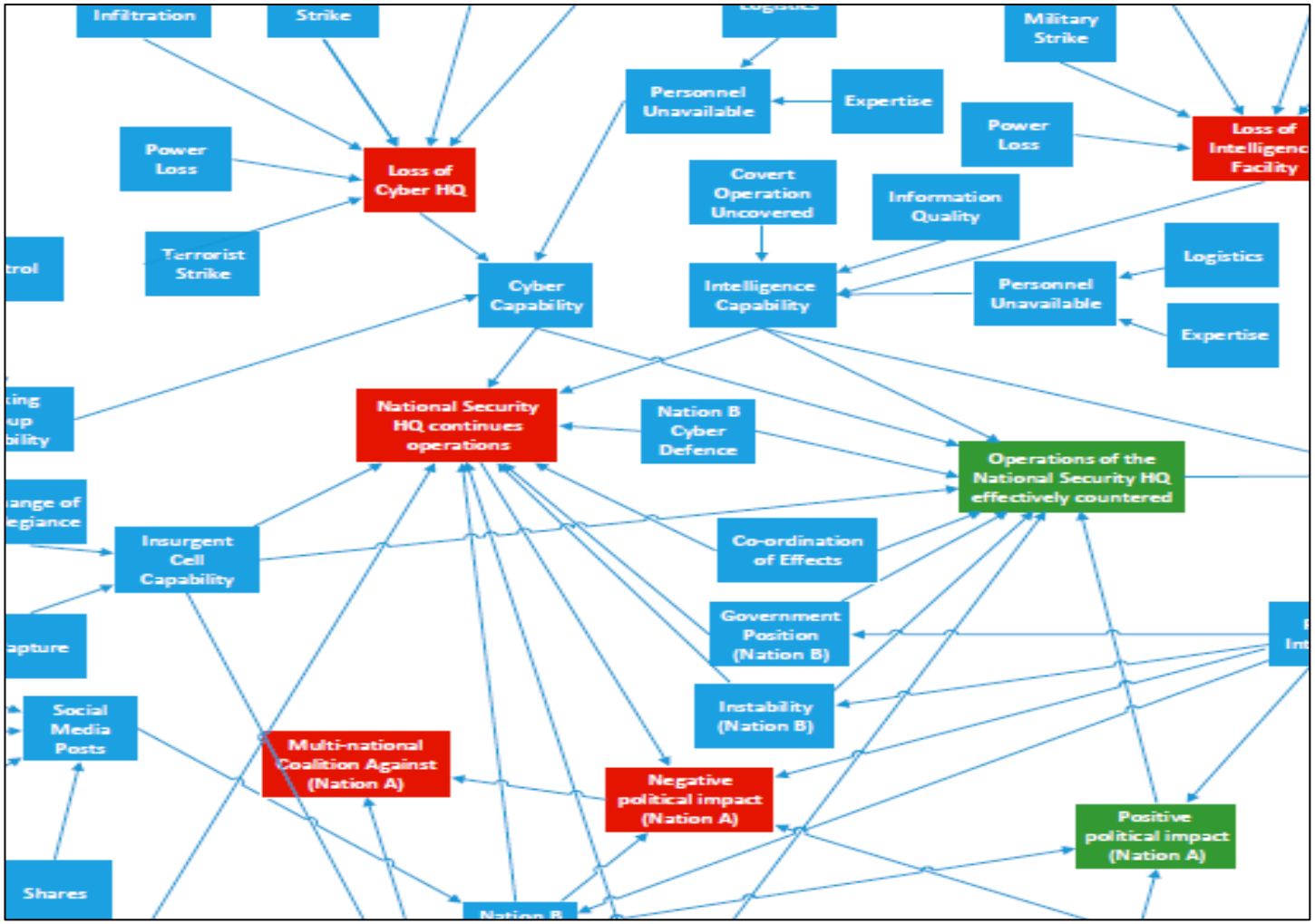
Hybrid Scenario Elements



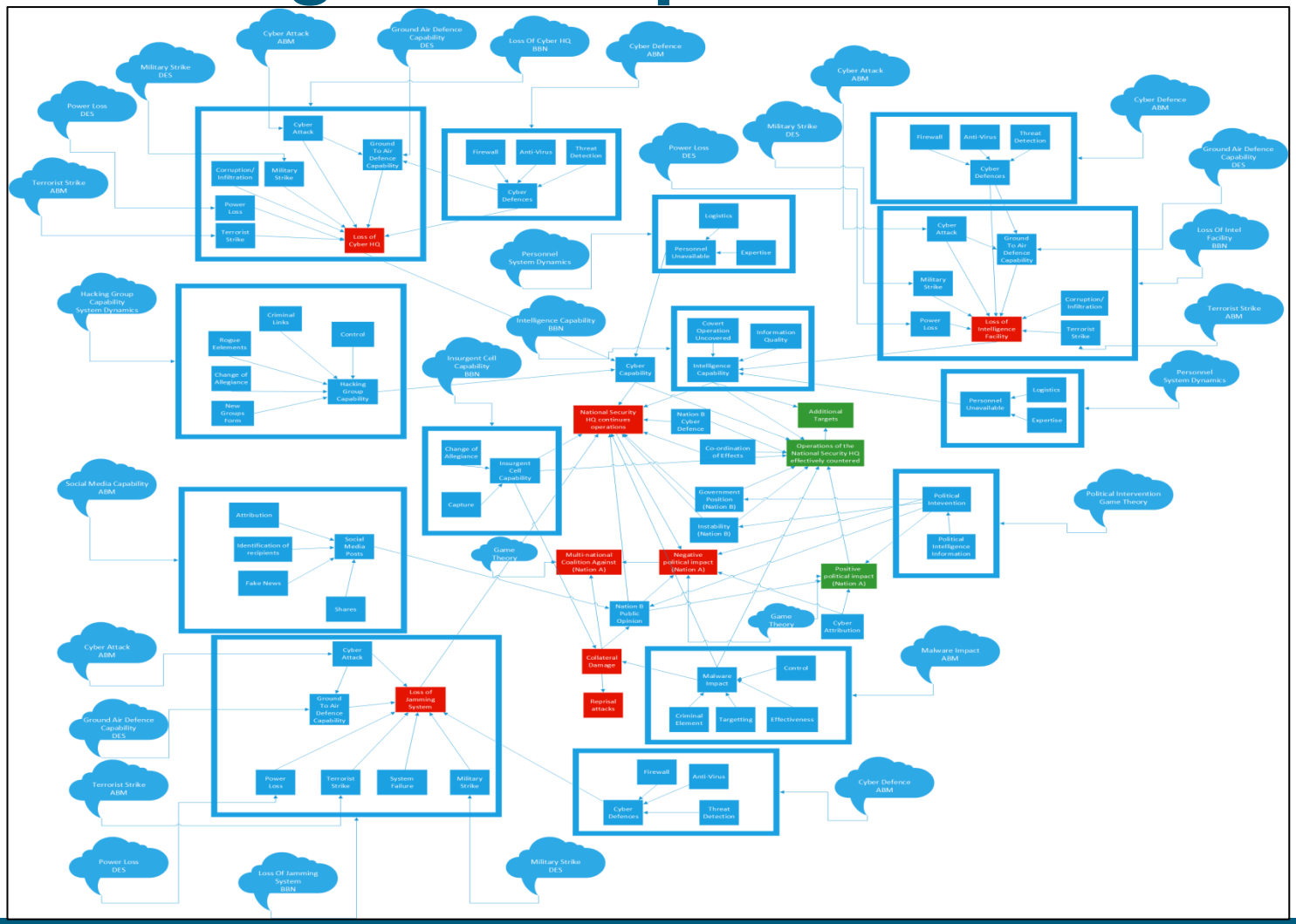
Non-Traditional Effects SoS Risk Causal Network



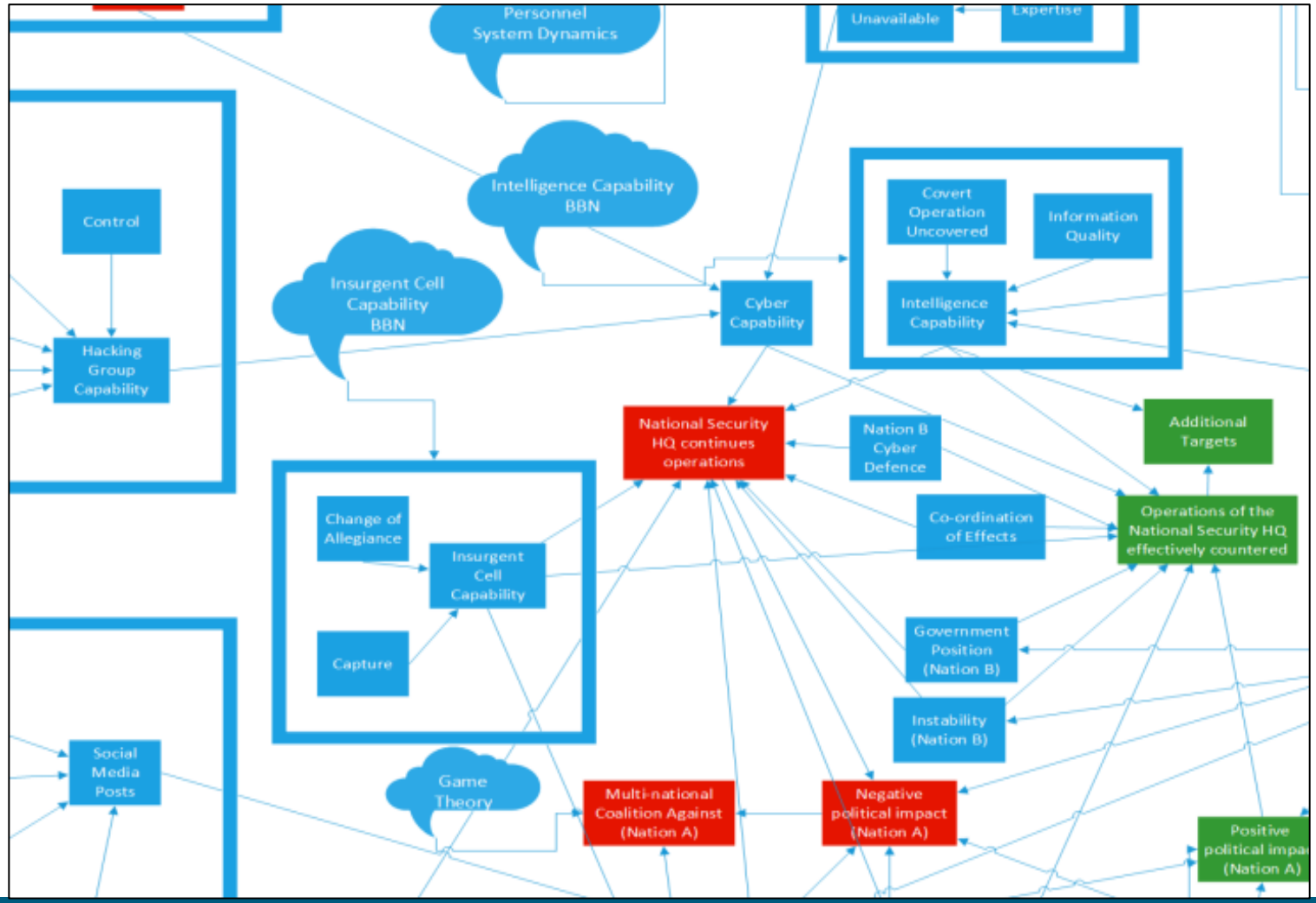
Non-Traditional Effects SoS Risk Causal Network



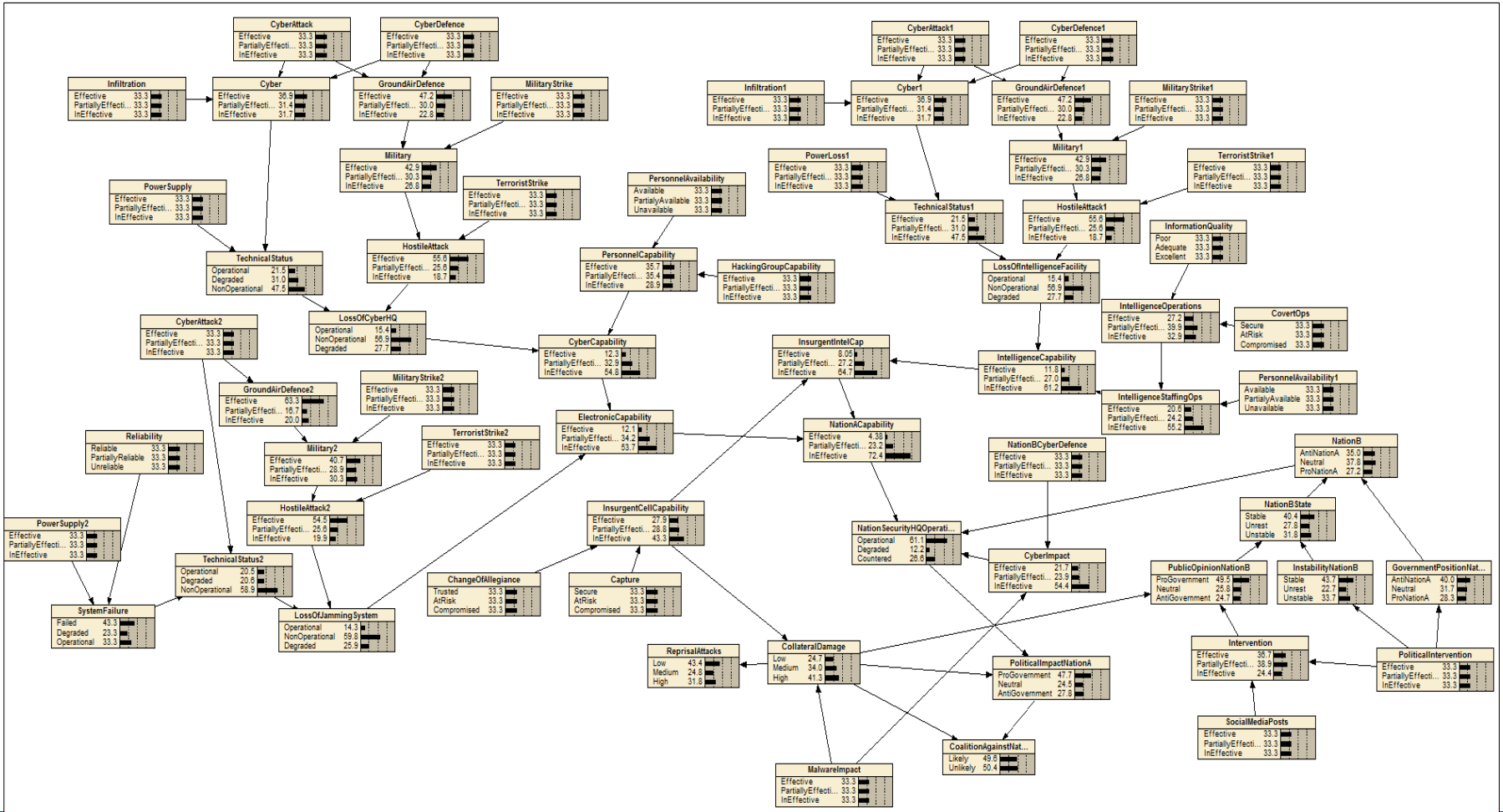
Modelling Technique Selection



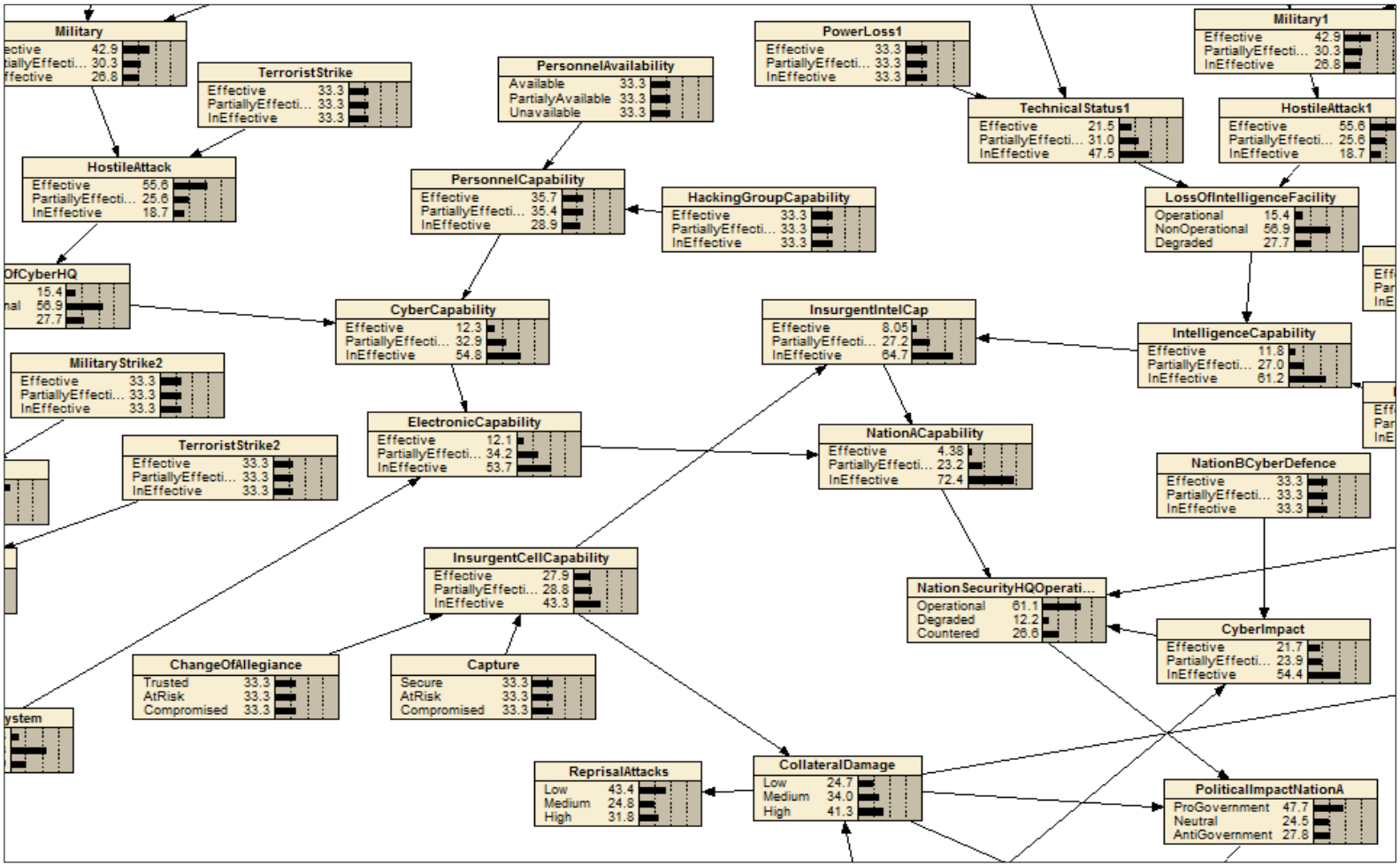
Modelling Technique Selection



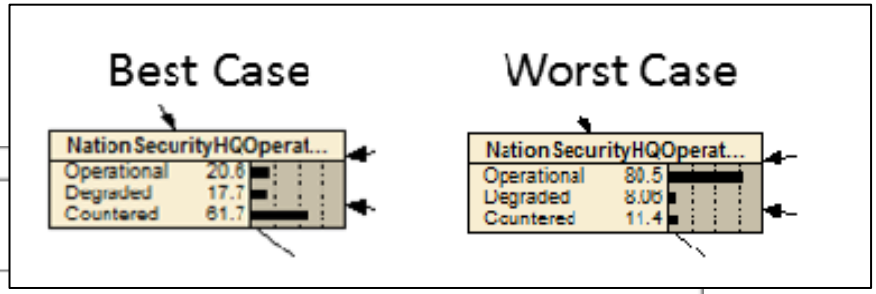
Bayesian Belief Network

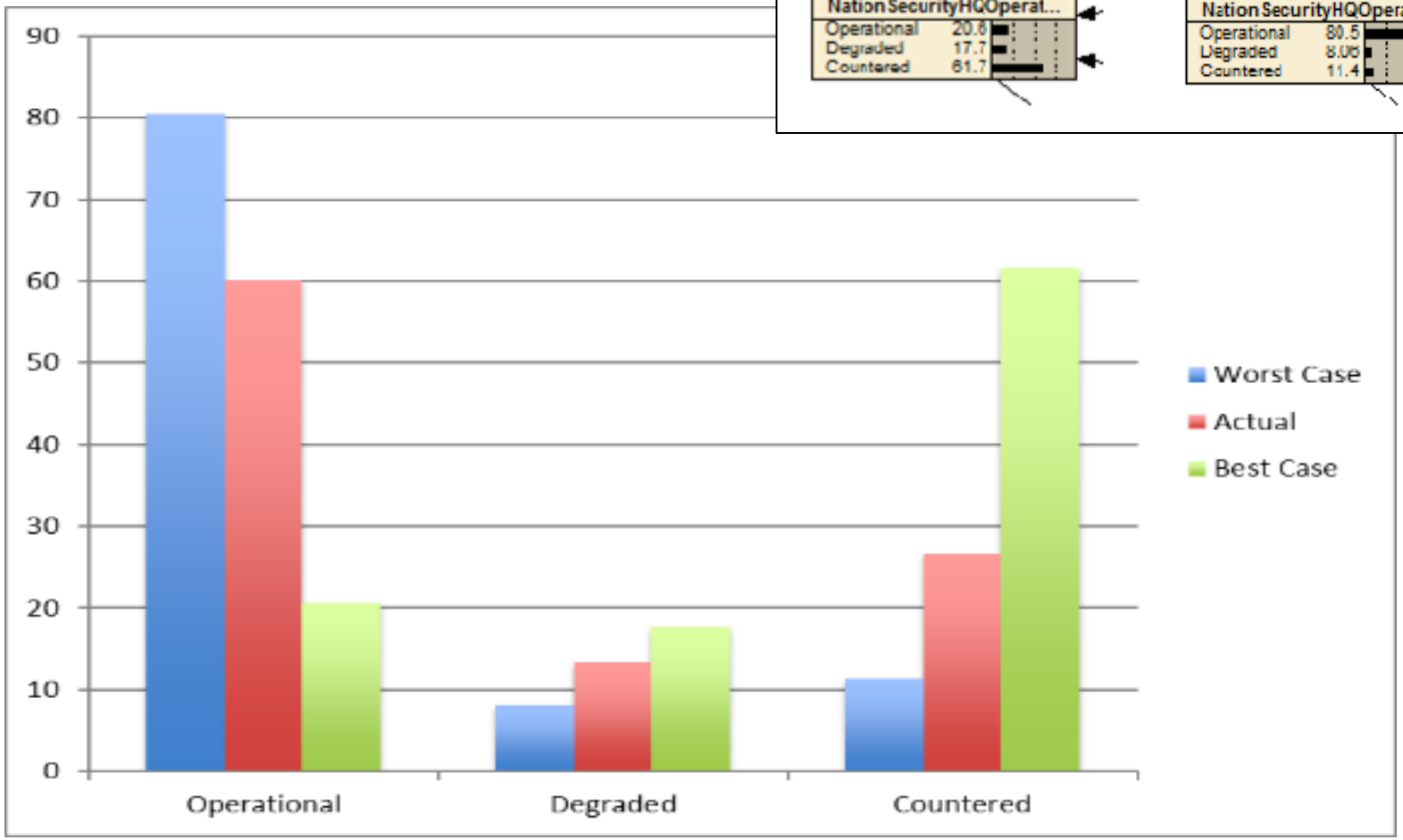


Bayesian Belief Network



Analysis





Future Exploitation

- Operational Decision Support
  - Full-Spectrum of Effects (Risks and Opportunities)
- Force Design
  - Balance of Investments (Traditional vs Hybrid)
- Agile C2 Training and Mission Rehearsal
  - Exercising and planning to use all capability levers
- War-gaming and Experimentation
  - Hybrid doctrine and tactics development
- Integration into M&S Ecosystem
  - NATO's M&S as a Service (MSaaS)

Conclusions

- The approach supports the integration of heterogenous models and simulations
  - Allowing hybrid scenarios to be represented comprehensively
- The analysis of multiple SoS allows identification of both operational risks or opportunities
  - Including potential attack vectors
- Due to the complex and heterogeneous nature of hybrid scenarios, effective modelling requires a range of techniques
  - Suitability of M&S techniques is determined by the problem context or focus
- A Bayesian modelling approach was found to be suitable for representing and analysing operational risk/opportunity
  - The post-Bayesian learning will improve further iterations and use
- The potential for exploitation of the approach is significant across defence applications
  - The modelling requirements are best achieved through integration through a M&S Ecosystem (e.g. MSaaS)

[dstl] Ministry of Defence

ATEQ Consulting

UK OFFICIAL

17 October 2019