

Paper 081

Using causal models to manage the cyber threat to C2 agility: working with the benefit of hindsight

Alex Barnett

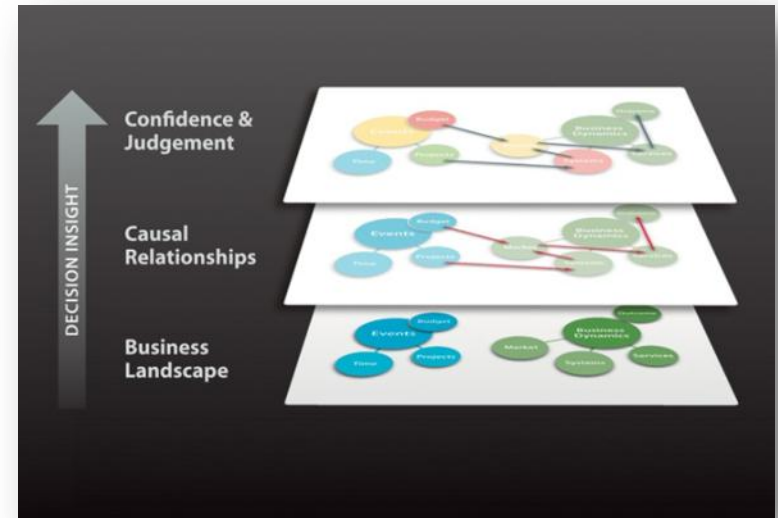
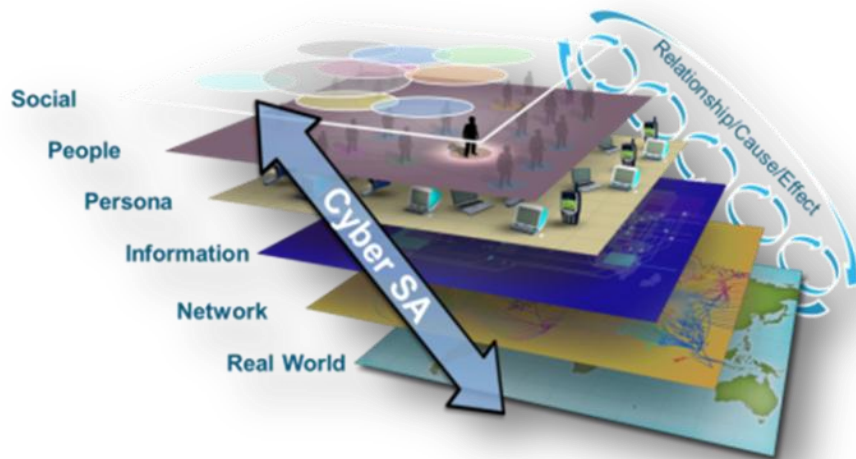
Simon Smith

Dick Whittington



Motivation – the complexity and causality of supporting military missions

- A *Causal Modelling* approach
- Projecting likely consequences of cyber events



Interactive cyber situational awareness: being mission focused & anticipatory

CONTROL



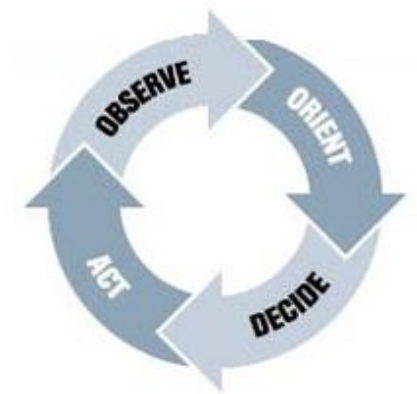
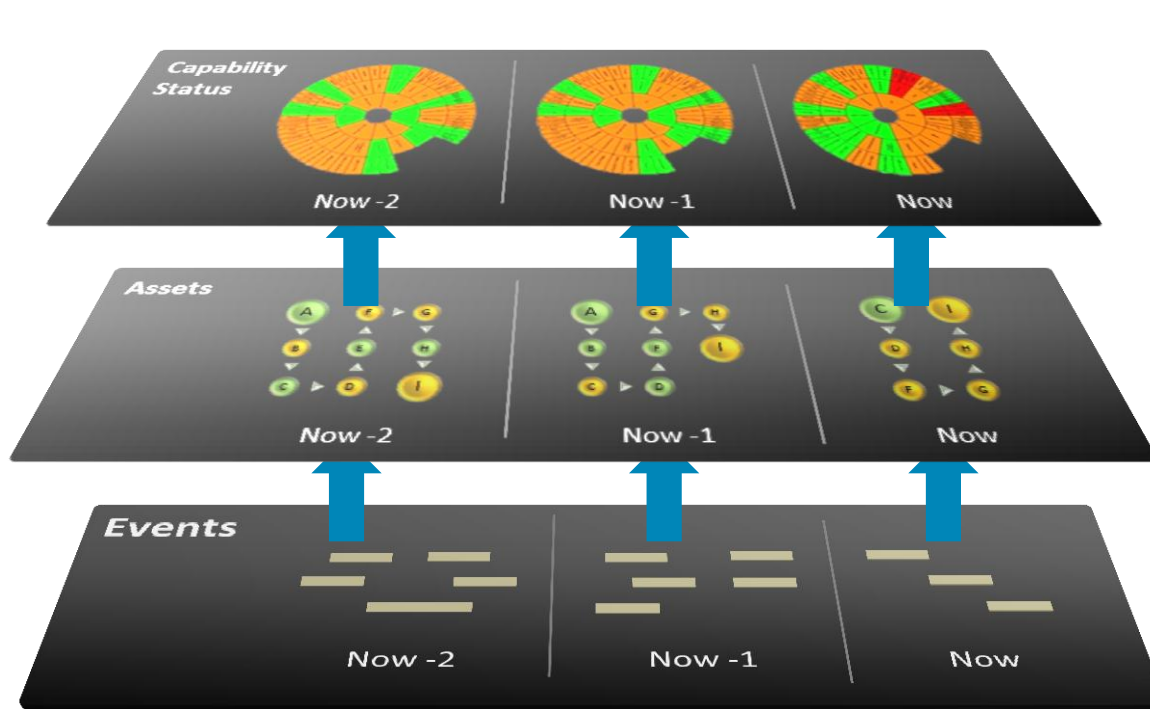
EVOLVE



OPTIMISE

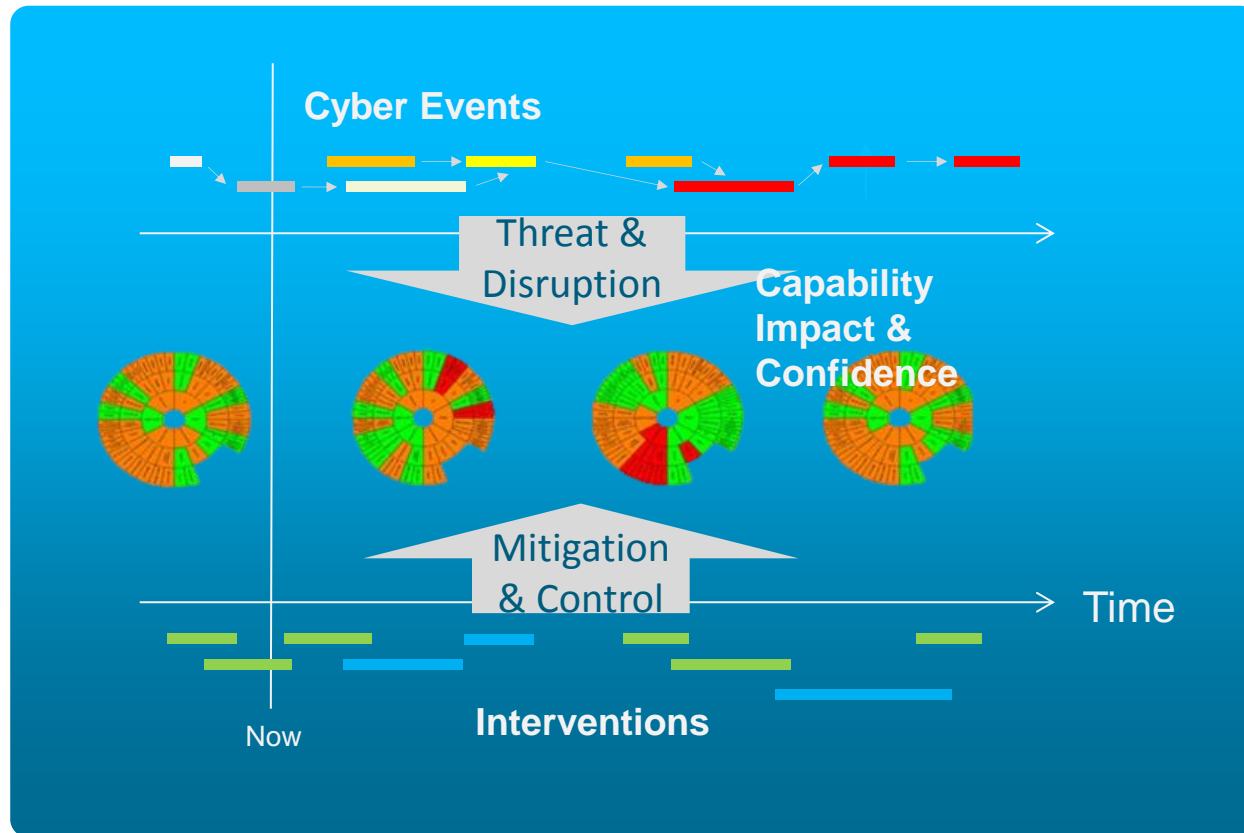


Linking underlying business processes to military effect in mission threads

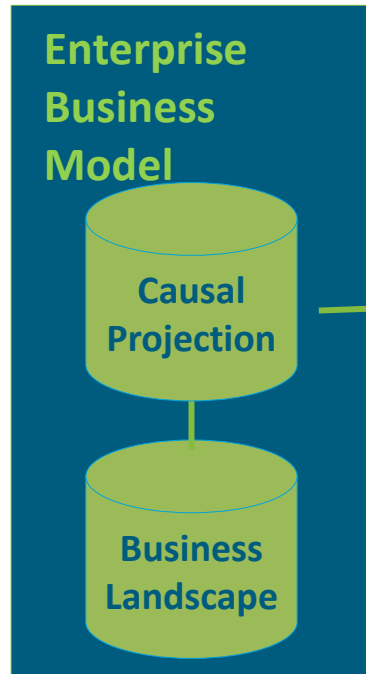


Classic OODA loop:
timely SA informs
“observe” and “orient”

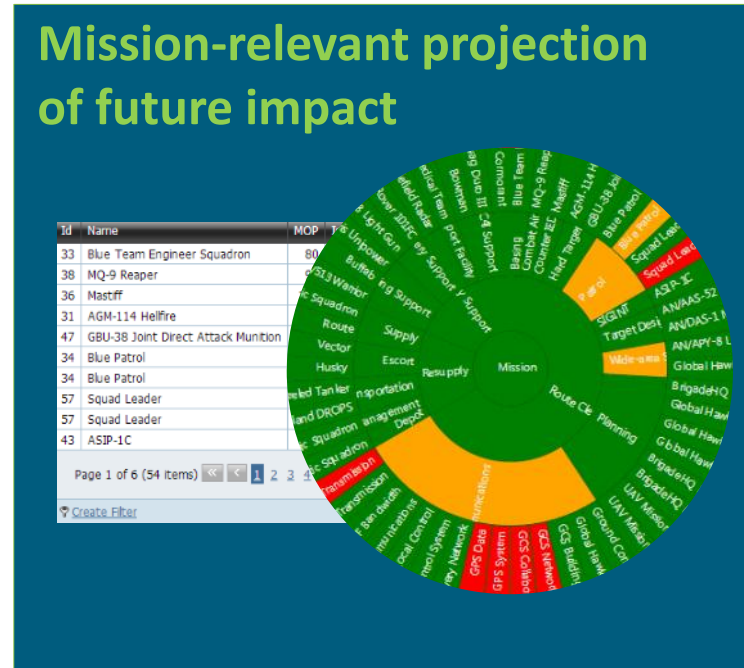
Identifying critical event chains and recommending intervention options



Cause & Effect dependency modelling

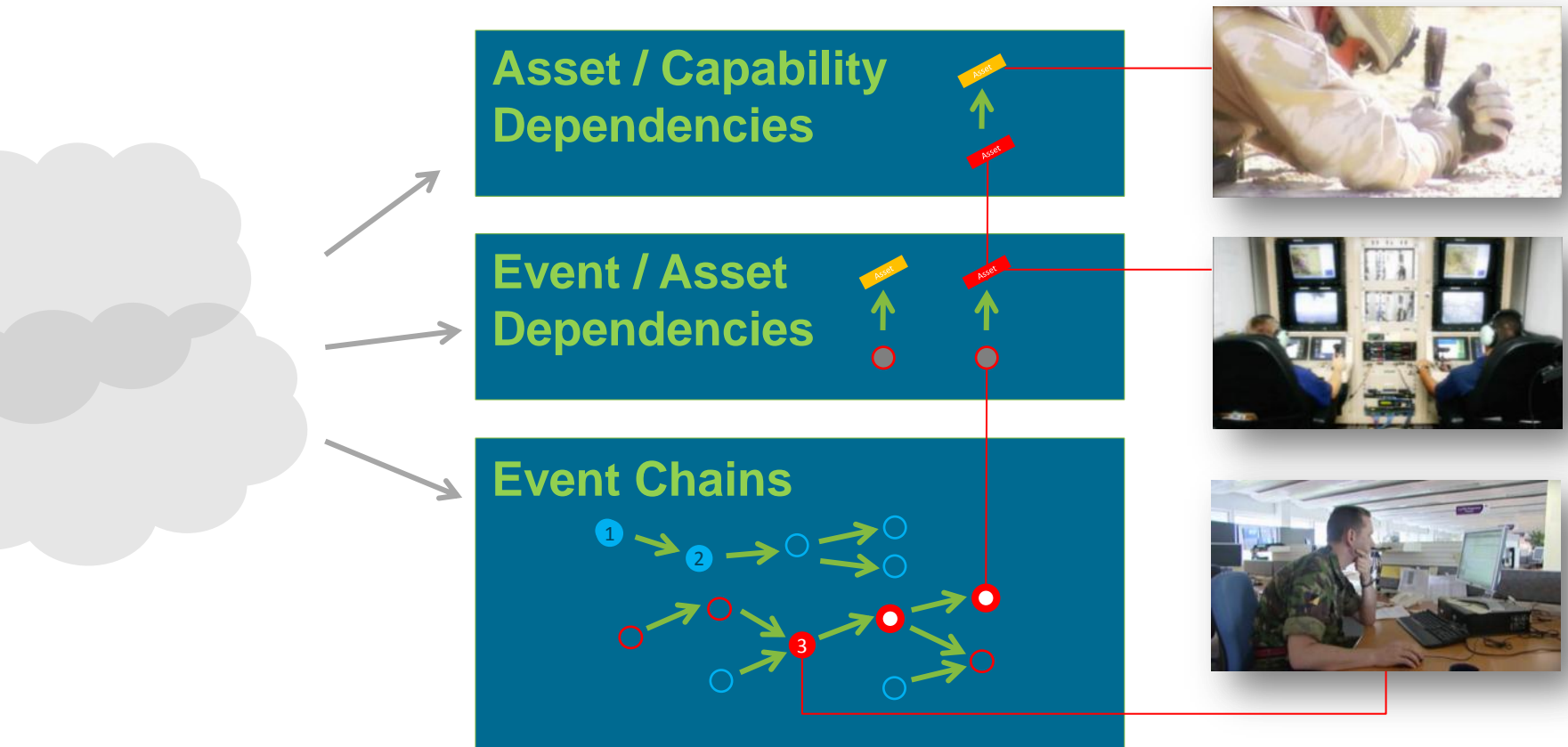


- Interpret
- Analyse
- Generate
- Track & Monitor

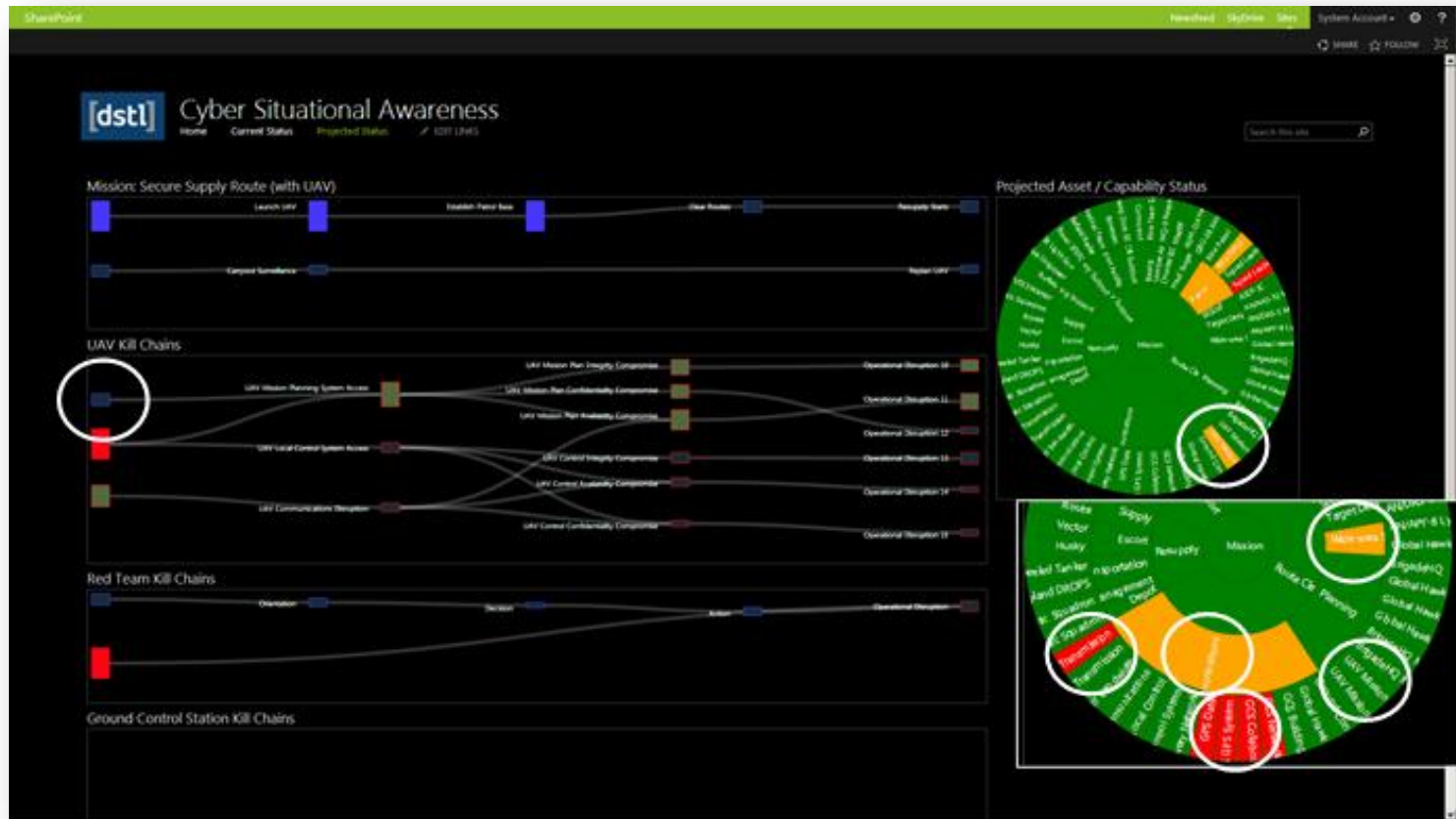


- Analyst Decisions
- Mission Commander Decisions

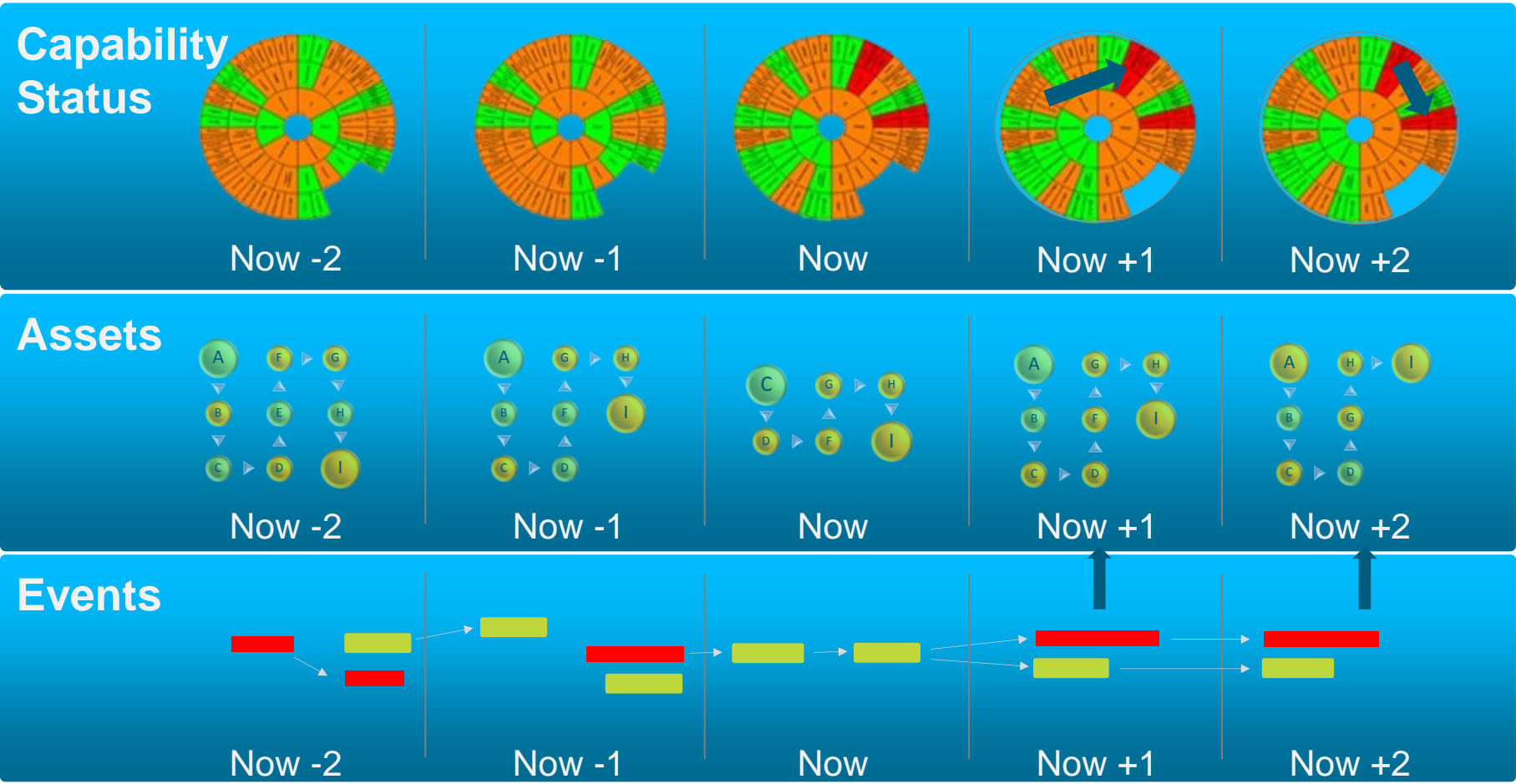
Enabling a **timely decision** by **presenting** the impact in an **actionable form**



Presenting the causal relationships and consequences to the mission commander



Next Steps – Projection into the future



Proactive decision making enabled by situational awareness and understanding

- Linking events to mission impact
- Identifying cause and effect critical points
- Presenting information to enable a timely decision



MooD
SMARTER DECISIONS

[dst1]

Questions?

