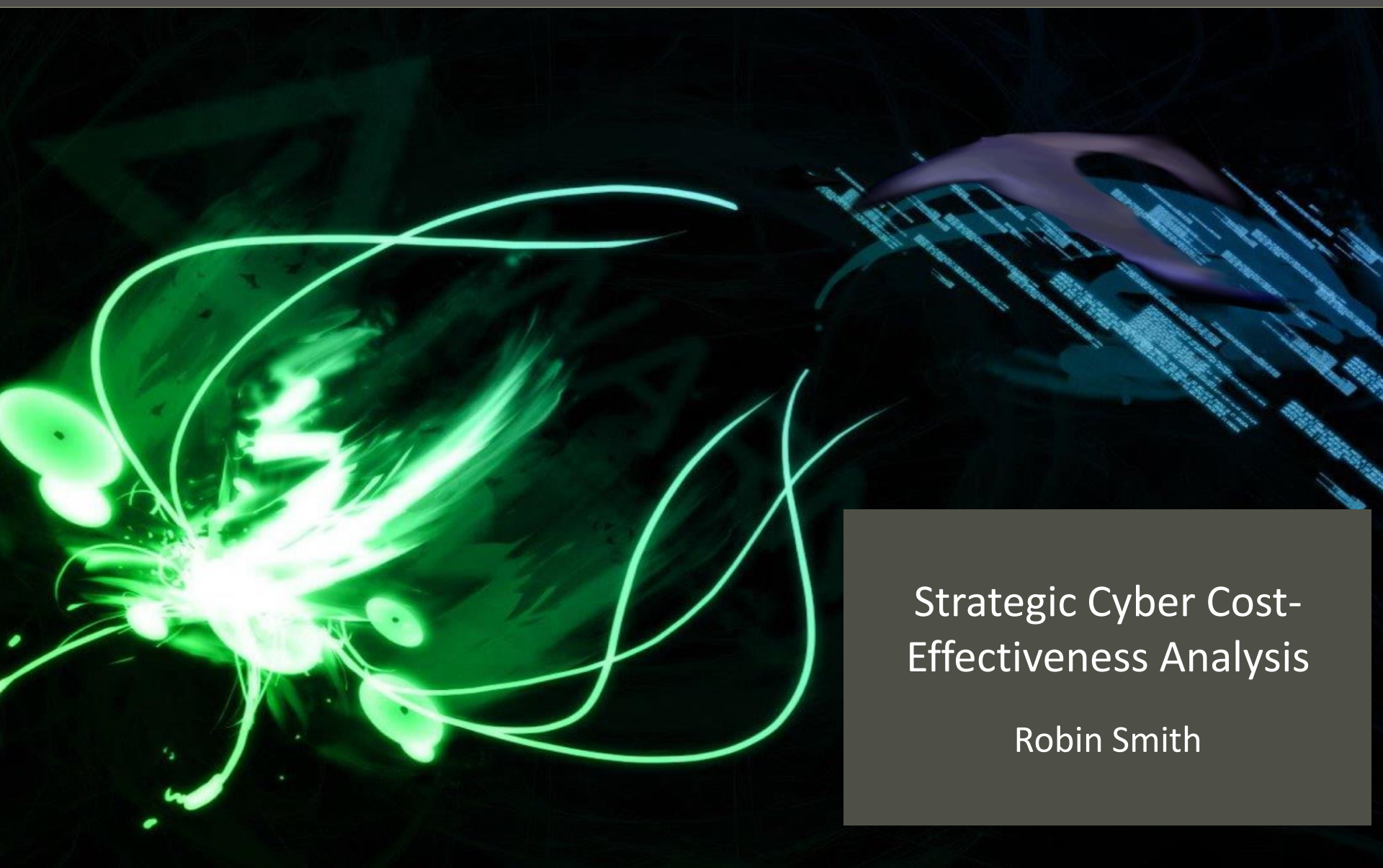




Arke Ltd



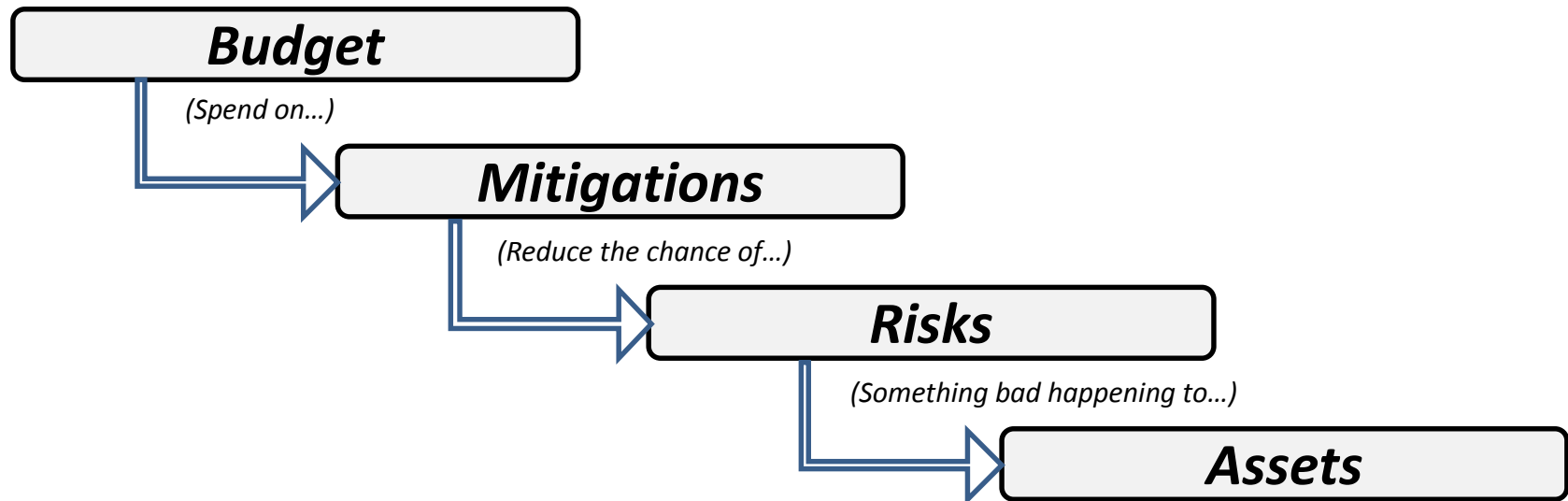
Strategic Cyber Cost-Effectiveness Analysis

Robin Smith

- Arke → Cost analysis, cost effectiveness and cost benefit
- Aim to present our thinking...
 - *Cost-Effectiveness/Cost-Benefit analysis of Cyber security...*
 - Different to the norm?
 - Interesting challenges?
 - How to address challenges?

To keep track:





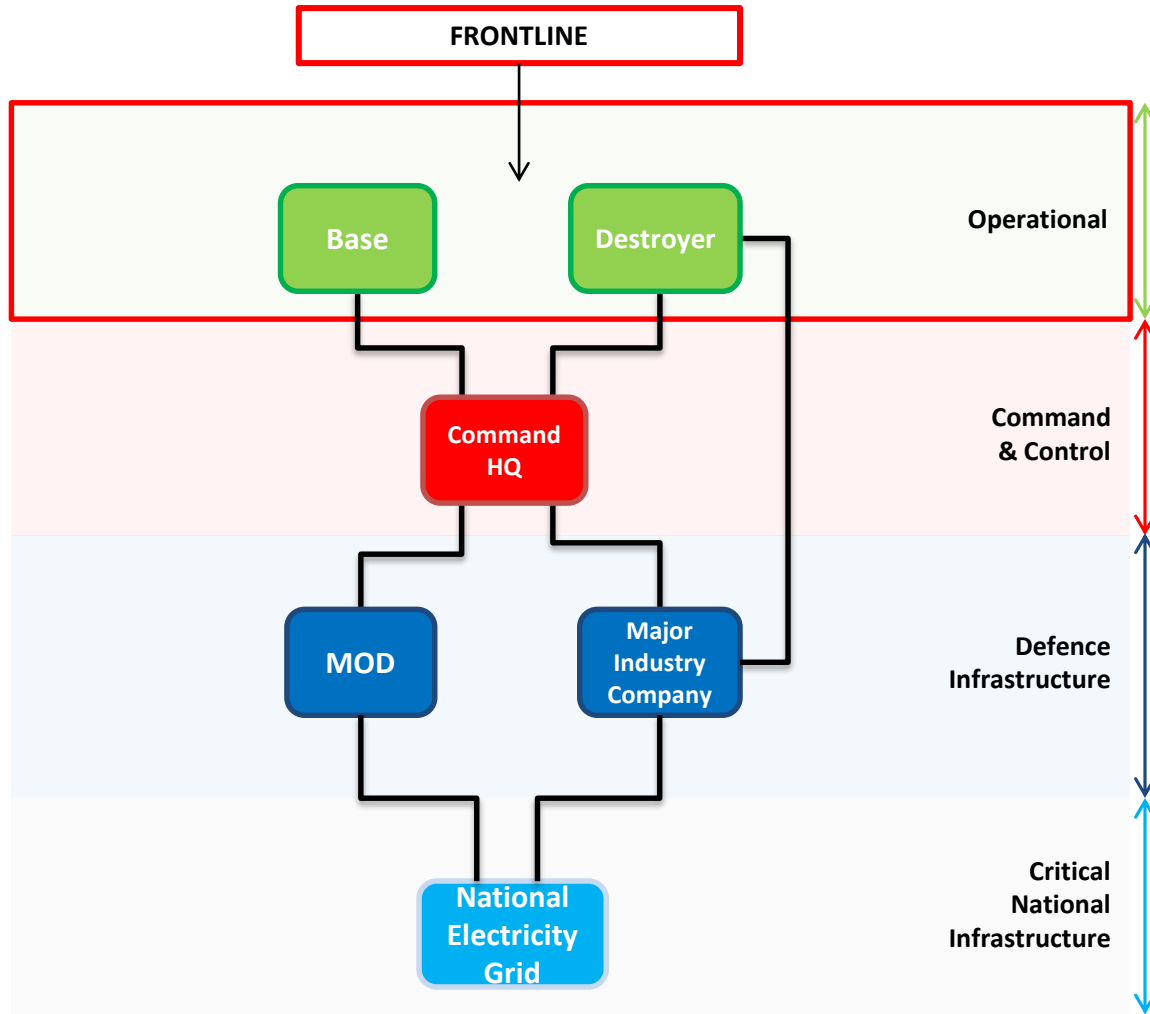
Key aspects for usual cases...

- Cost-Effectiveness directly related → **value for money** for taxpayer
 - Through defence perspective
- Assets → Entirely defence
- Assets → Not necessarily interconnections/interdependencies

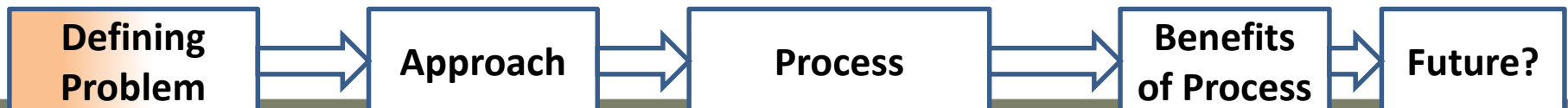


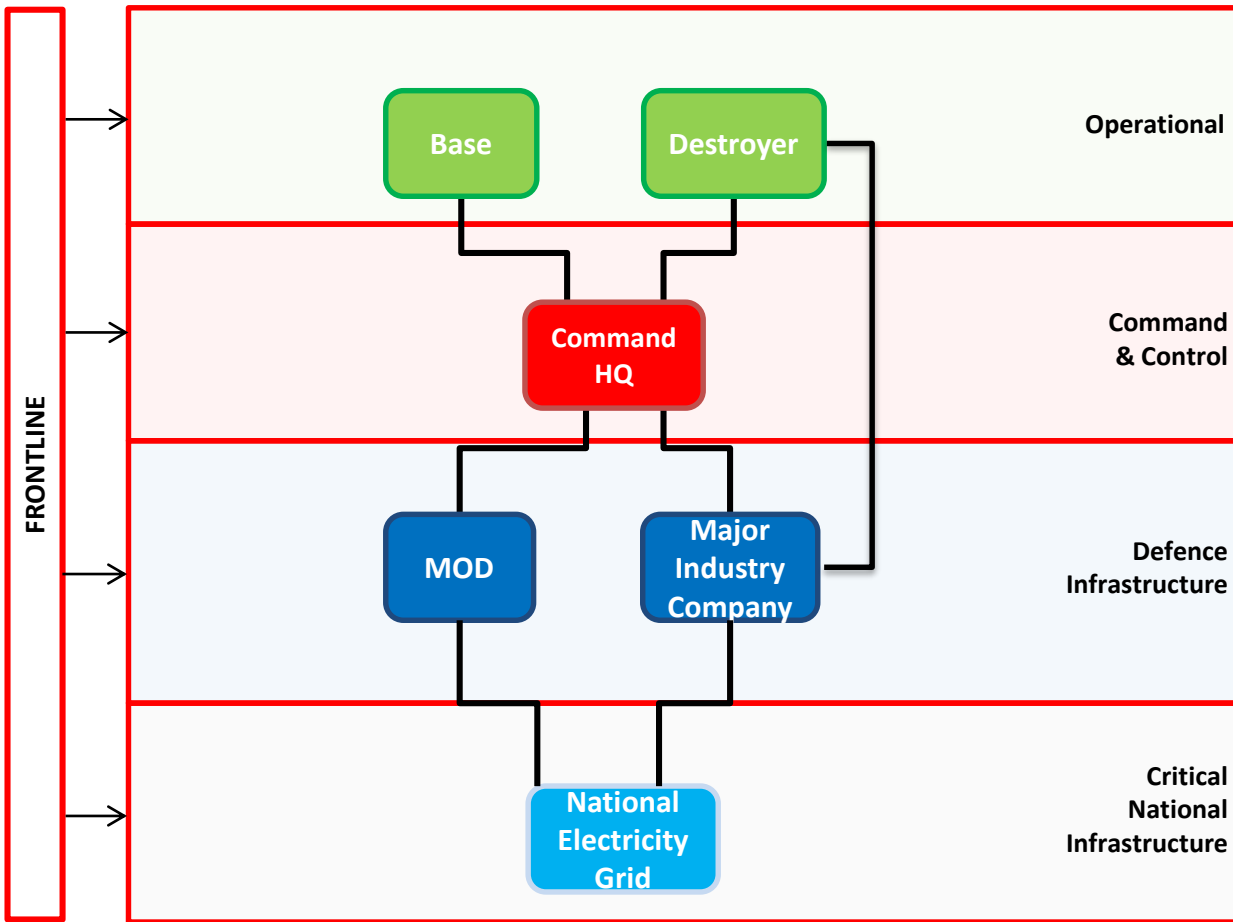


Assets and Infrastructure: Strategic Level



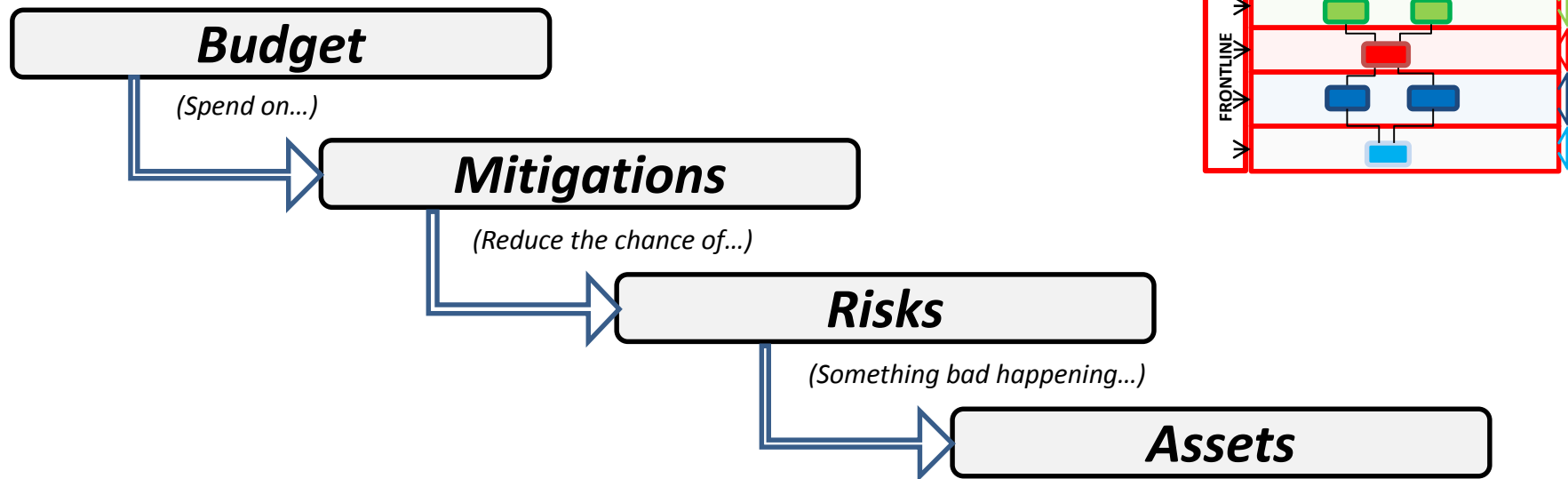
- Representation:
 - Network of nodes
- Nodes layered from the fighting end to the infrastructure that it depends upon in the long term
- Usually, risk of 'attacks' considered at the operational end.





- Representation:
 - Network of nodes
- Nodes layered from the fighting end to the infrastructure that it depends upon
- Communication with each other and some might depend on others to function
- Usually, risk of attacks considered at the operational end.
- All exposed to cyber security risks





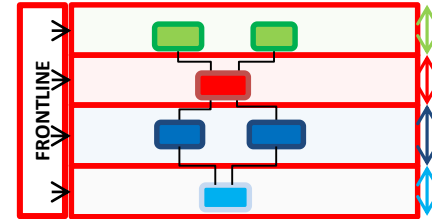
Key aspects for cyber security...

- Cost-Effectiveness directly related → **value for money** for taxpayer
 - Through defence, **trade, energy.. Etc.**
- Assets → Not all entirely Defence
- Assets → Have interconnections/interdependencies



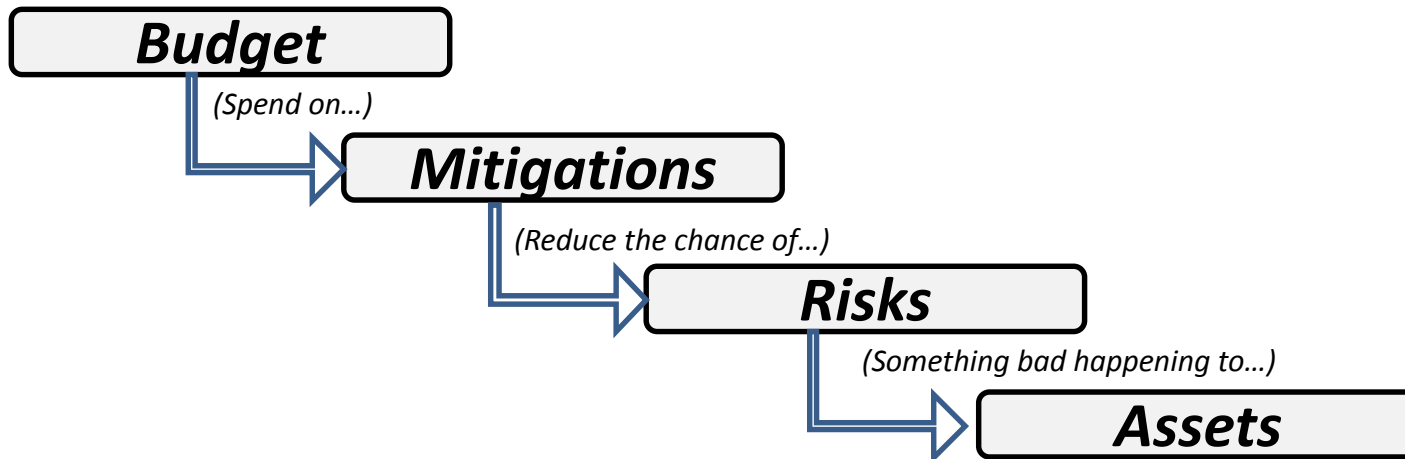
New problems with cyber security

1. Wider Impacts (than just defence)
2. Risks propagate (between nodes)



High-level understanding → Best way to spend money?

- On reducing chance of successful cyber attacks



Influencing our approach

Challenges

- Wider Impacts (than just military)

- Reflect principles of assessing risks to information systems in the UK
- “HMG Information Assurance Standard 1 – Technical Risk Assessment” (Government Standard) for information system risk assessment
- Assess core goals of Information Assurance separately
 - *Confidentiality* -> Loss of privacy
 - *Integrity* -> Loss of trust
 - *Availability* -> Loss of presence
- Assess relevant impact categories separately (‘Business Impact Levels’) e.g.
 - *Military Operations*
 - *Trade*
 - *Energy... etc.*



- ① • **Quantifying Risks**
 - ① ○ *CHANCE* of a successful attack
 - ② ○ *IMPACT* of a successful attack
- ② • **Effectiveness of mitigations**
 - Highest ***reduction in probability*** of successful attack
 - (want to reduce risks where they have a ***high impact***)
- ③ • **Cost**
 - ① ○ Estimated costs of ***implementing mitigations***
 - ② ○ Estimated costs of ***risks affecting nodes***



1 Quantifying Risks

① CHANCE of a successful attack

- Probability of successful attack – based on...
 - different parameters for different risks
- Example *Risks* could be quite different

Indicative Parameters

1.	<i>Compromised Hardware</i>	->	<i>quantities procured, percentage compromised</i>
2.	<i>IP Theft</i>	->	<i># of people security cleared, percentage threats</i>
3.	<i>DOS attack – national scale</i>	->	<i>SME judged /work-shopped quantities?</i>

- Parameters may have different values for each node in the network



1 Quantifying Risks

① CHANCE of a successful attack

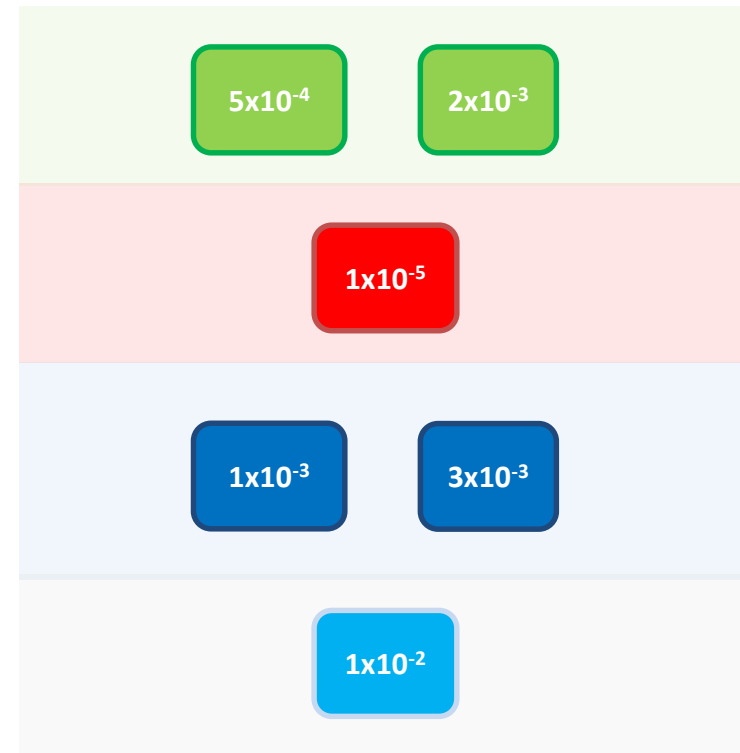
- Uncertainty – MUST capture the ‘error margins’
 - Three point estimating
 - E.g. ‘Best Case’, ‘Most Likely’, ‘Worst Case’ → Weighted mean value
 - Manually set distributions – eliciting uncertainty
- Range of inputs
 - Background work → through to → best judgement
- Identify and engage relevant Subject Matter Experts



1 Quantifying Risks

① CHANCE of a successful attack

Nodes: Risk 1



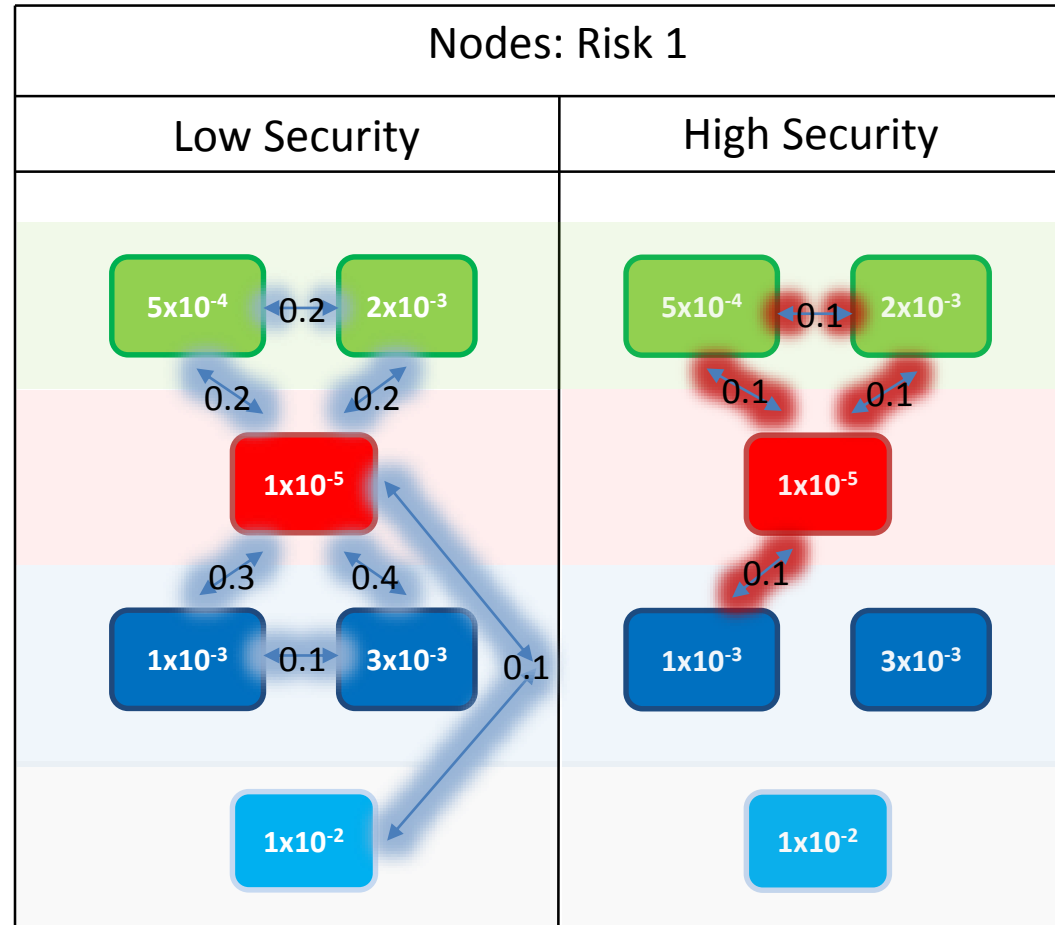
Risk Propagation - problem

- For Risk x
 - Mean probability of occurrence at each node
- **Usually**
 - (unmitigated) probabilities of occurrence
 - 'at risk' assets not connected
- **Cyber**
 - consider propagation of risks
 - 'at risk' assets are connected



Risk Propagation - treatment

- Two connection types?
- **Conditional probabilities**
 - Per risk per connection?
 - Two-way value, or one-way values?
- Implications
 - Simulation/modelling of probability
 - Triggers an impact at the node



1 Quantifying Risks

① CHANCE of a successful attack

- **Summary – CHANCE of a successful attack**
 - Detailed/not detailed info on risks
 - Capture uncertainty
 - Probabilities of Propagation
 - Use Subject Matter Expert judgement (where needed)



1 Quantifying Risks

⑥ IMPACT of a successful attack

Impact

- How bad is the loss of an asset?

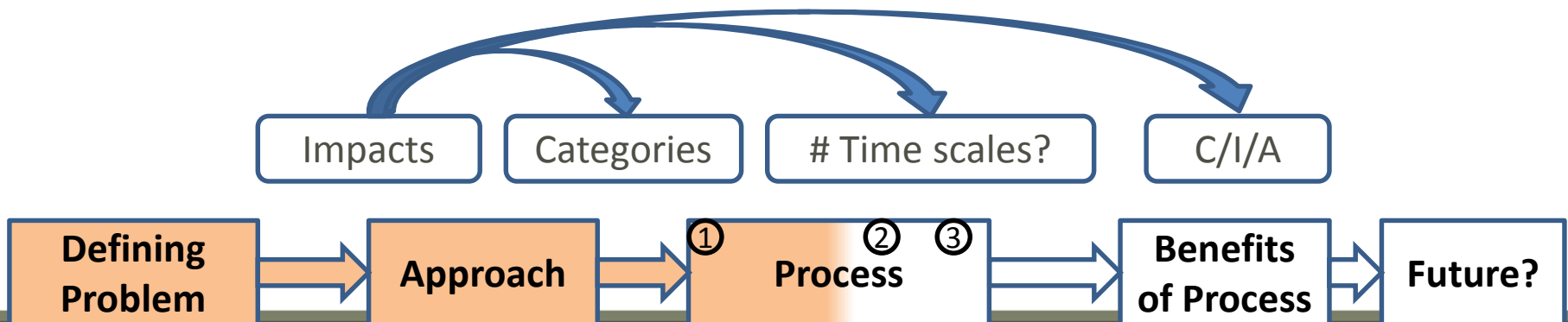
1. **Categories** e.g. ...

- Military Operations
- Trade
- Energy

2. **Time scale**

3. **Confidentiality, Integrity or Availability**

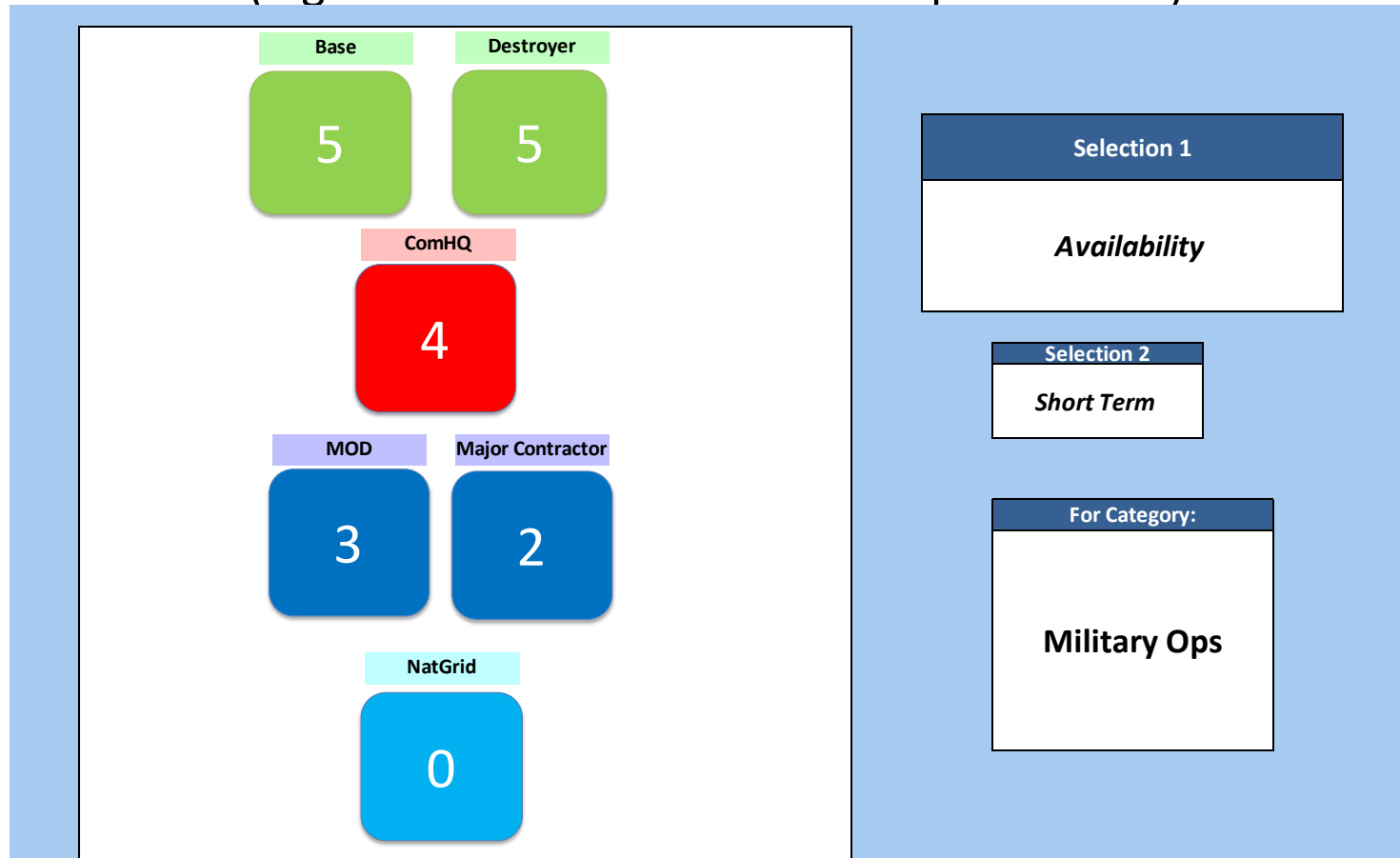
(loss of privacy, loss of trust, loss of presence)





1 Quantifying Risks

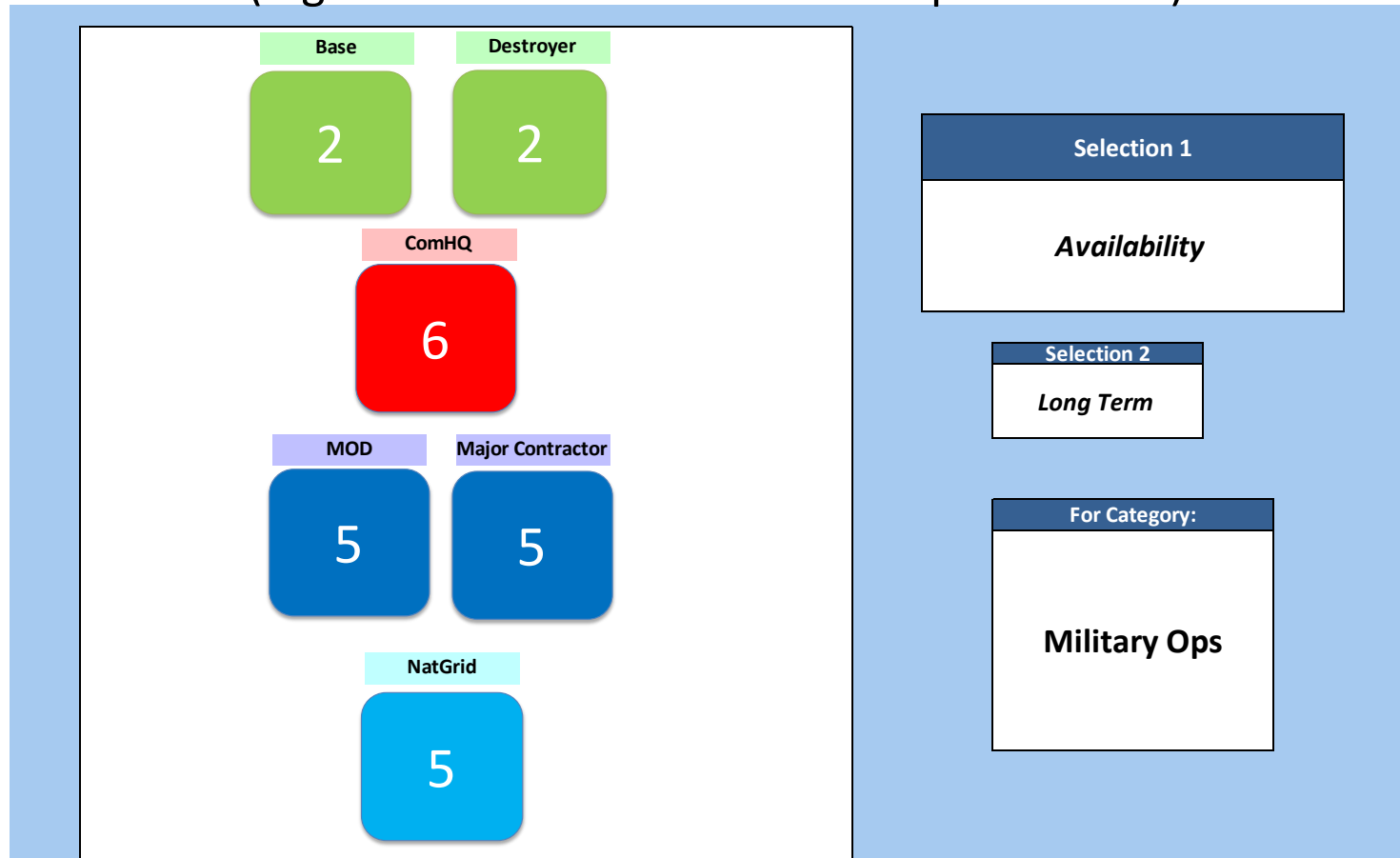
- What is the impact of a successful attack?
 - Score 0→6 (e.g. consistent with 'Business Impact Levels')
- ⑥ IMPACT of a successful attack





1 Quantifying Risks

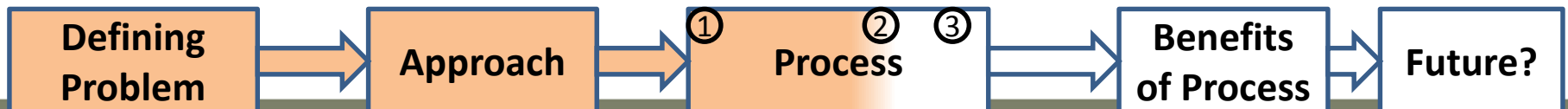
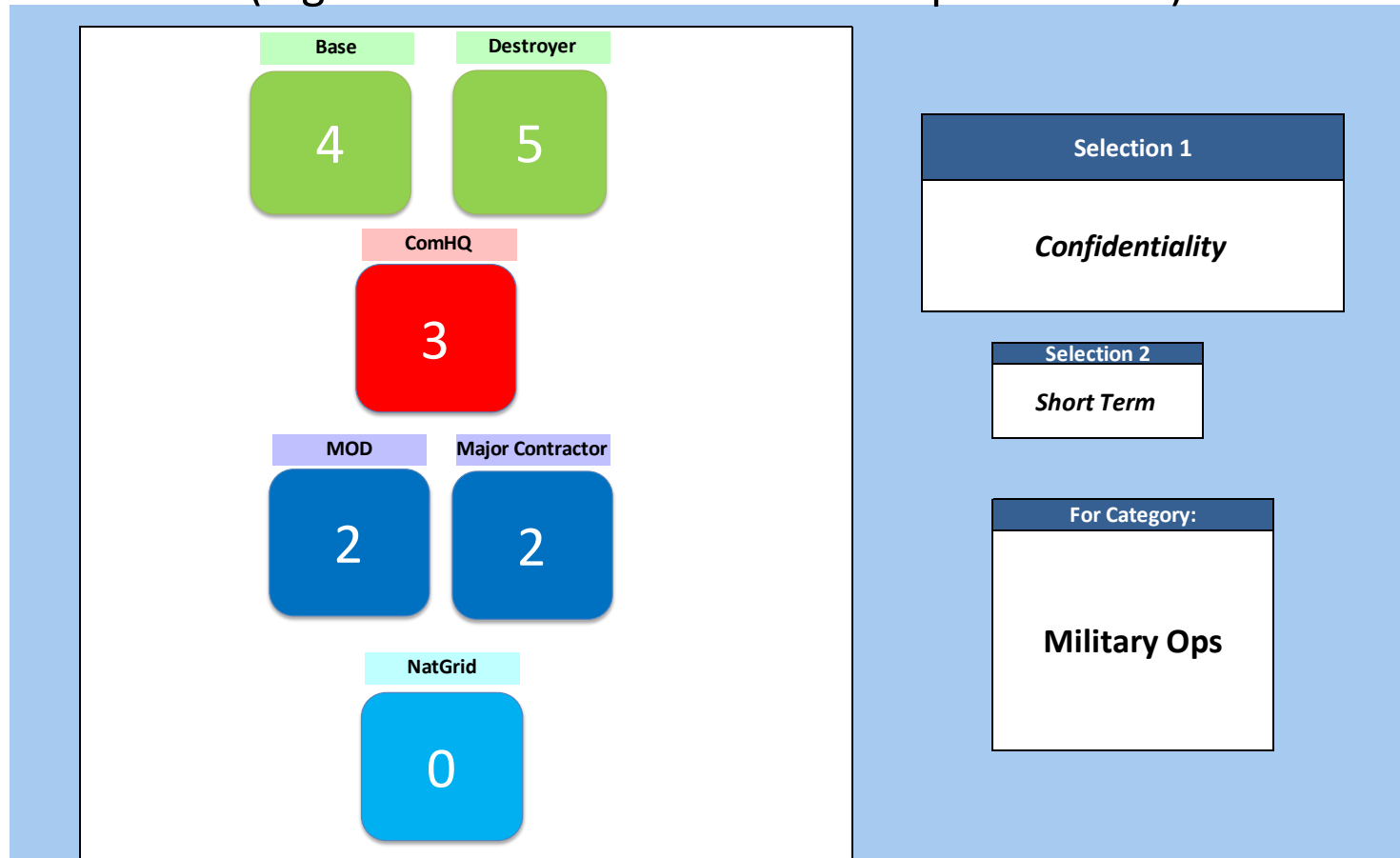
- What is the impact of a successful attack?
 - Score 0→6 (e.g. consistent with 'Business Impact Levels')
- ⑥ IMPACT of a successful attack





1 Quantifying Risks

- What is the impact of a successful attack?
 - Score 0→6 (e.g. consistent with 'Business Impact Levels')
- ⑥ IMPACT of a successful attack



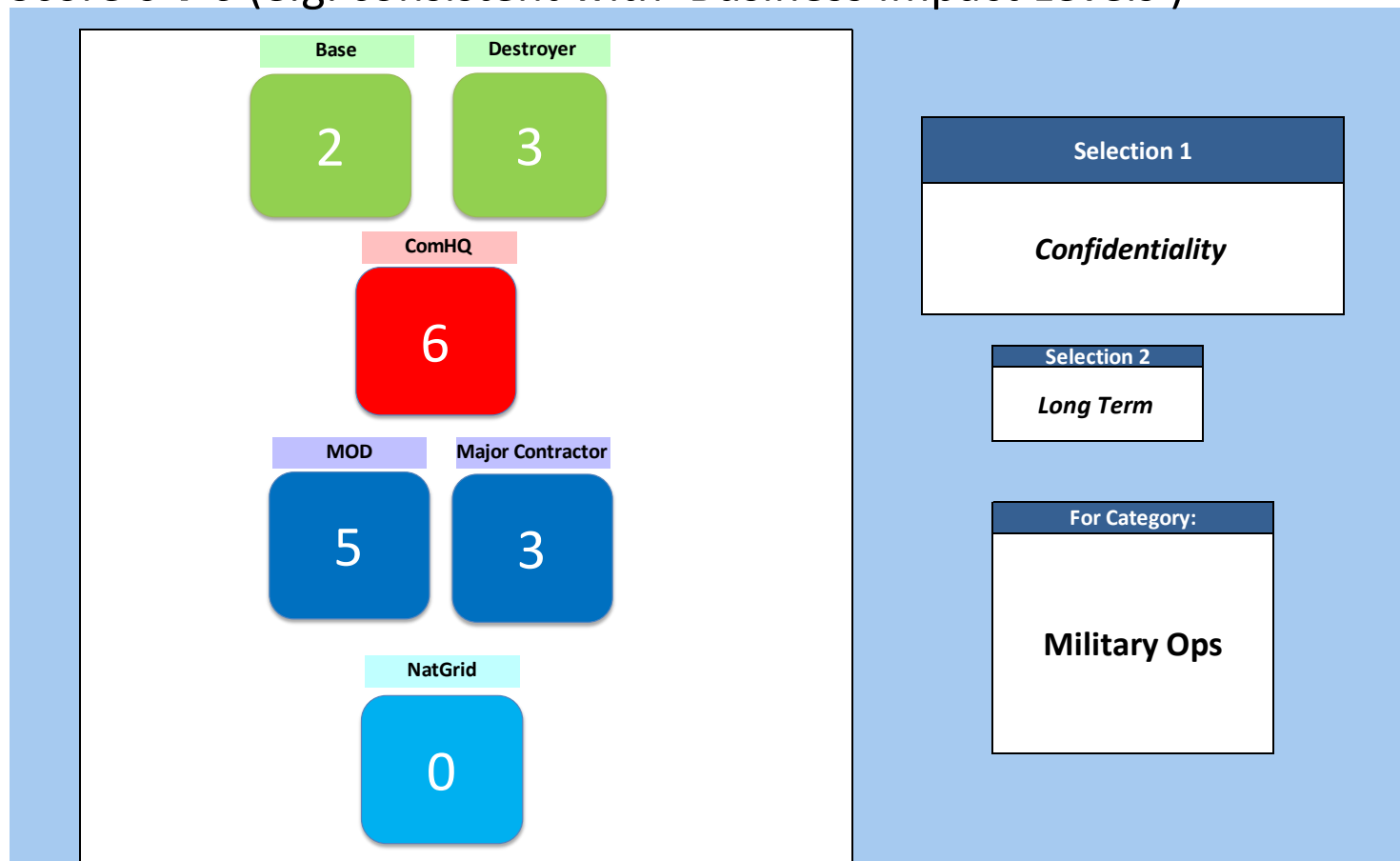


1 Quantifying Risks

- What is the impact of a successful attack?

⑥ IMPACT of a successful attack

- Score 0→6 (e.g. consistent with 'Business Impact Levels')



1 Quantifying Risks

⑥ IMPACT of a successful attack

- **Summary – IMPACT of a successful attack**
 - Minimum information to capture wider impacts:
 - Categories
 - Time Scales
 - Confidentiality, Integrity, Availability



2

- **Effectiveness of mitigations**

- How much does **CHANCE** of a successful attack **decrease**?
- (how high an impact might there be if attack is successful)

- Similar to assessing **CHANCE of a successful attack...**

- **Summary –**

- Detailed/not detailed info on mitigations
 - Capture uncertainty
 - Probabilities of Propagation
 - Use Subject Matter Expert judgement (where needed)



- ③ • **Costs**
 - ③ ○ Estimated costs of *implementing mitigations*
 - ③ ○ Estimated cost impact of *risks affecting nodes*

- Q. How complex might the estimating be?



③ Mitigations

e.g.

1. Reduce chance of an Edward Snowden?
 - *Interview all personnel with security clearance X, every 5 years*
2. Reduce chance of buying compromised hardware?
 - *Set up and run an organisation to scrutinise imports*

Estimate cost of implementing

- Not too difficult
- Based on people and effort?





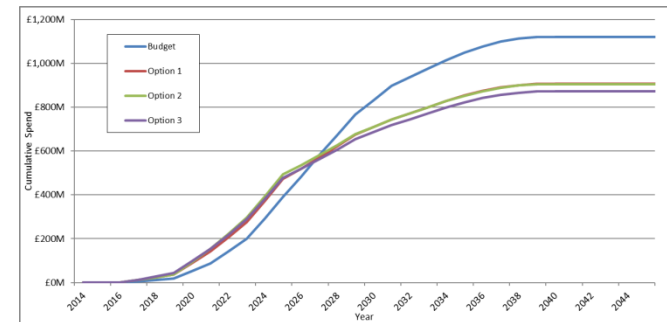
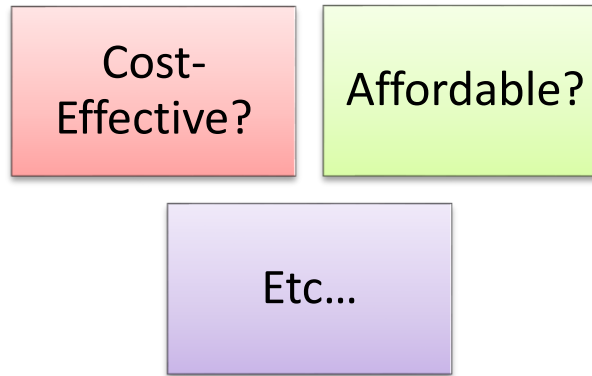
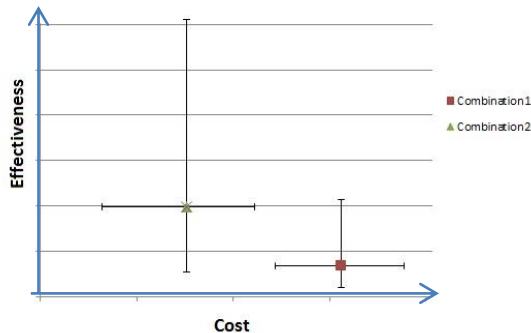
- ⑥ • **Cost ‘impacts’ of a successful attack**
 - **What is the cost of losing an asset (for each ‘C/I/A’ property)**

CIA	Data Sources		Issues
	Military	Non-Military	
Availability (loss of presence)	Country Force Structure Cost Model, military accounts (e.g. UINs)	Overheads from company accounts	Time-related Short and Long term costs of running the asset (inc. existing response information system staff etc.)
Confidentiality (loss of privacy)	!	!	Loss of profit, re-development costs of exposed research, very uncertain
Integrity (loss of confidence)	!	!	E.g. Battlefield pictures untrustworthy. Difficult to define, proportion of availability/confidentiality?



• Summary of Process

- Describe Assets (at high level) – network of nodes
- Quantify Risks
- Quantify Mitigation Actions
- Quantify Costs
- Feed information into a tool → assess most cost-effective combinations of mitigations



- *Same outputs for cyber security, by the approach discussed?*



- **Benefits**

- Audit trail for the evidence
- Quickly assess alternative combinations of mitigations
- Engage stakeholders – buy-in?
- A Tool allows: Evolving Threat, Learning Curves in Mitigation
- Assess at different levels of detail
- Run strategic-level ‘attack’ scenarios

- ***Applicable to cyber security, by the approach discussed?***



- **Future Effort**

- Risk Propagation
 - Test methods of simulation
- Cost Impacts
 - Estimating ‘loss of trust’, ‘loss of privacy’
- Example framework
- Example tool
- Scalability?
 - Easy/fast to add risks?
 - Easy/fast to add nodes (to the network of assets)?

