Including Cyber Defence in the High Level Analysis process.

Colin Irwin

Dstl Policy & Capability Studies

August 2013

Long term vision

- *To establish provision for Cyber Defence as part of the mainstream departmental planning*
- Have objective, robust, *routine* analytical representation of:
  - Threats;
  - Risks & benefits;
  - Force Structure implications;
  - and costs of Cyber Defence.
- *Just like any other capability.*

The problem

- Need to compare this....

The problem

- Few opponents can pose a serious conventional threat to western forces;
- But potentially low cost of entry to the cyber arena places it within the grasp of almost anyone.
- *Protecting UK forces against hostile cyber operations is not an option but a necessity.*
- Realising that we need to do *something* is only the first step. We need to determine *what* we need to do.

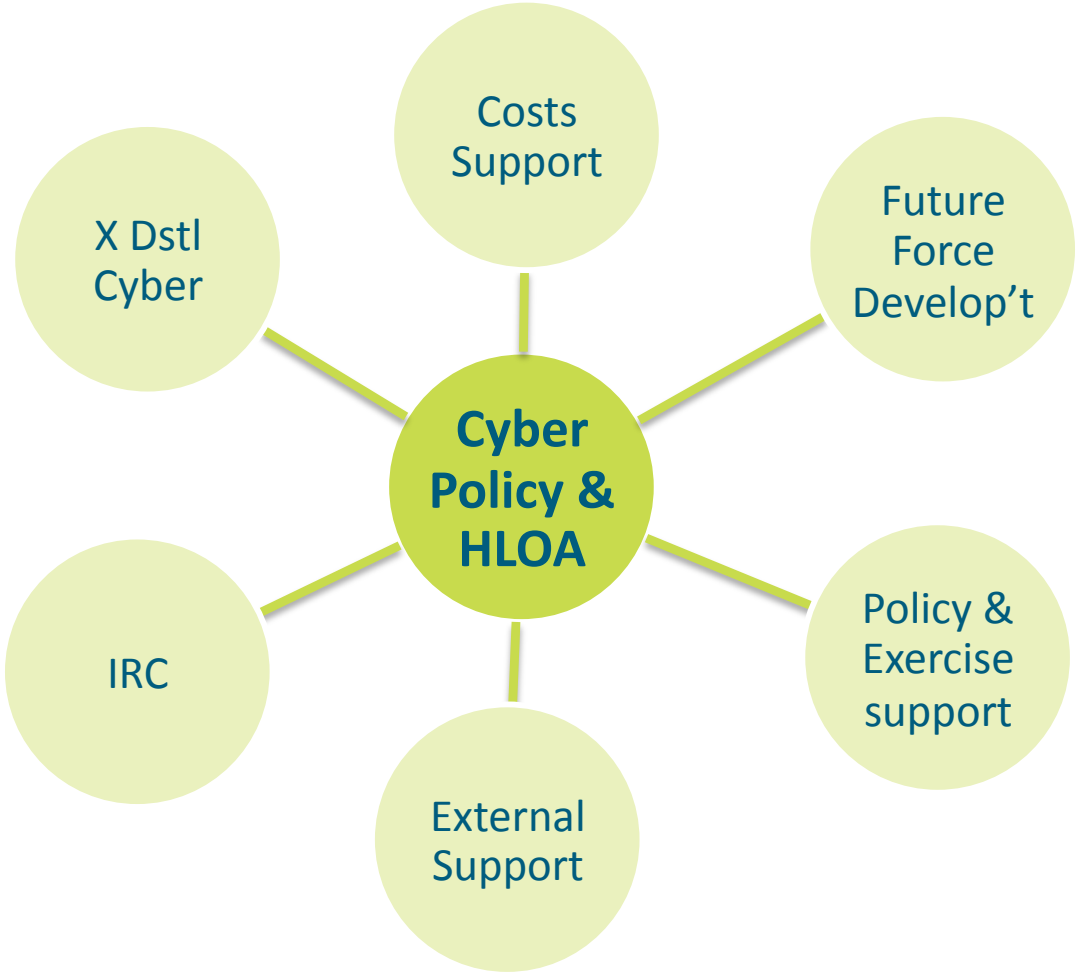
Need analysis to give advice on:

- How developments in cyber potentially impact:
  - C2 capabilities;
  - “Conventional” capabilities;
  - Full range of likely future operations (home and abroad);
  - Business-As-Usual.
- Understanding risks.
- Understanding feedback mechanisms.
- Aggregation of impact.
- Costs - financial and other.

Simple?

- Substantial effort has been invested in understanding cyber capabilities.
- But this has not yet been well integrated into the mainstream High Level Operational Analysis (HLOA) programme.
- However it does mean that there is something to build on.

PCSD Cyber Hub and Spoke



PCSD Cyber Hub and Spoke

Cyber Policy & HLOA

- Cyber Policy Support
- Dynamic Modelling
- Force Development
- Cyber Scenarios
- Force Structures
- Manning
- Costs

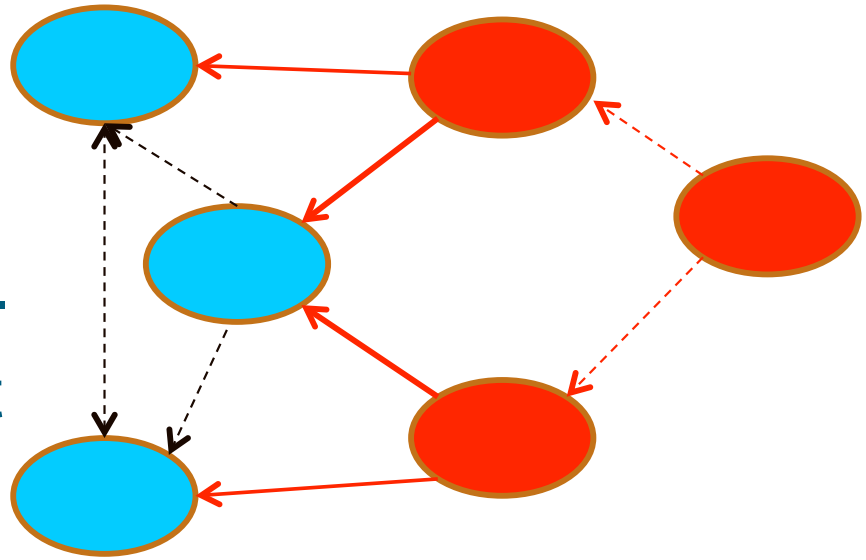
Cyber Policy Support

- Support to MOD Cyber Policy in their production of a Cyber Strategy, including:
  - Cyber and Deterrence;
  - Cyber and Early Intervention;
  - ‘Cyber Littorals’.

- In-year, ad-hoc support to Cyber PoI and DCDC on cyber policy issues of immediate concern.
  - E.g. assessment of ‘The Global Cyber Game’.

Dynamic Modelling of Cyber Defence

- Constructed initial influence diagram model of how we believe the different elements of cyber interact.
- Provides context to examine specific questions.
- Potential wide range of uses.
- Populating it not straightforward.
- Exploring potential development through, e.g. MARVEL.

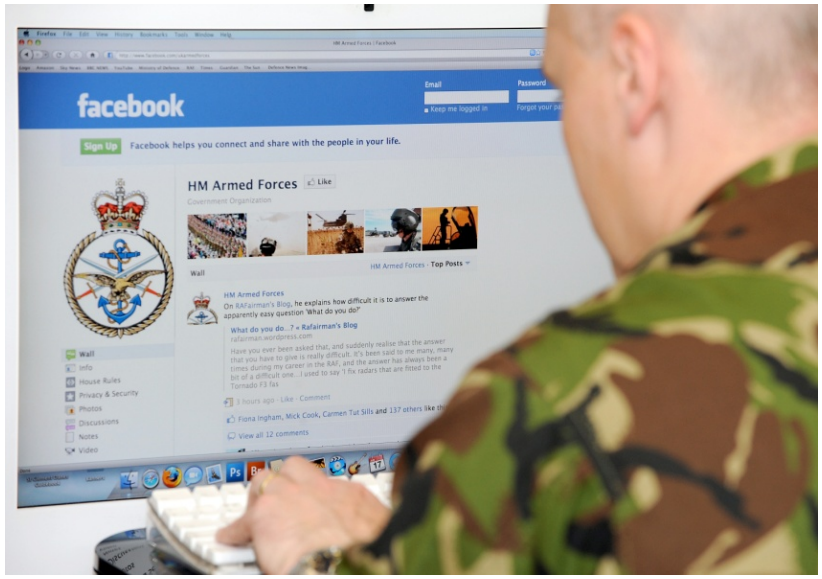


Future Force Development

- Existing process to inform full spectrum of UK Force Development.
- Scenario-based planning and analysis.
- Examining from Cyber Defence perspective:
  - Threats;
  - Requirements.

Cyber Scenarios

- Develop a set of scenarios through which the utility of different Cyber Defence capabilities can be explored.
- Some capabilities can be explored in the existing planning scenarios.
- But additional scenarios needed to explore the full spectrum of cyber threats and defence requirements.



Force Structures

- The MOD is developing force structures to deliver and sustain Cyber Defence capabilities as part of Future Force 2020.
- Scarce cyber resources will be centrally managed to enable prioritisation:
  - Defence Cyber Operations Group (DCOG) within Joint Forces Command.
- Is this enough? Appropriate?

Manning Requirements

- Aim is a tool that allows an informed estimate of the manpower required to undertake a series of defensive actions in cyberspace:
  - Given tasks derived from scenarios;
  - Given force structure.
- Feed into Costs analysis.

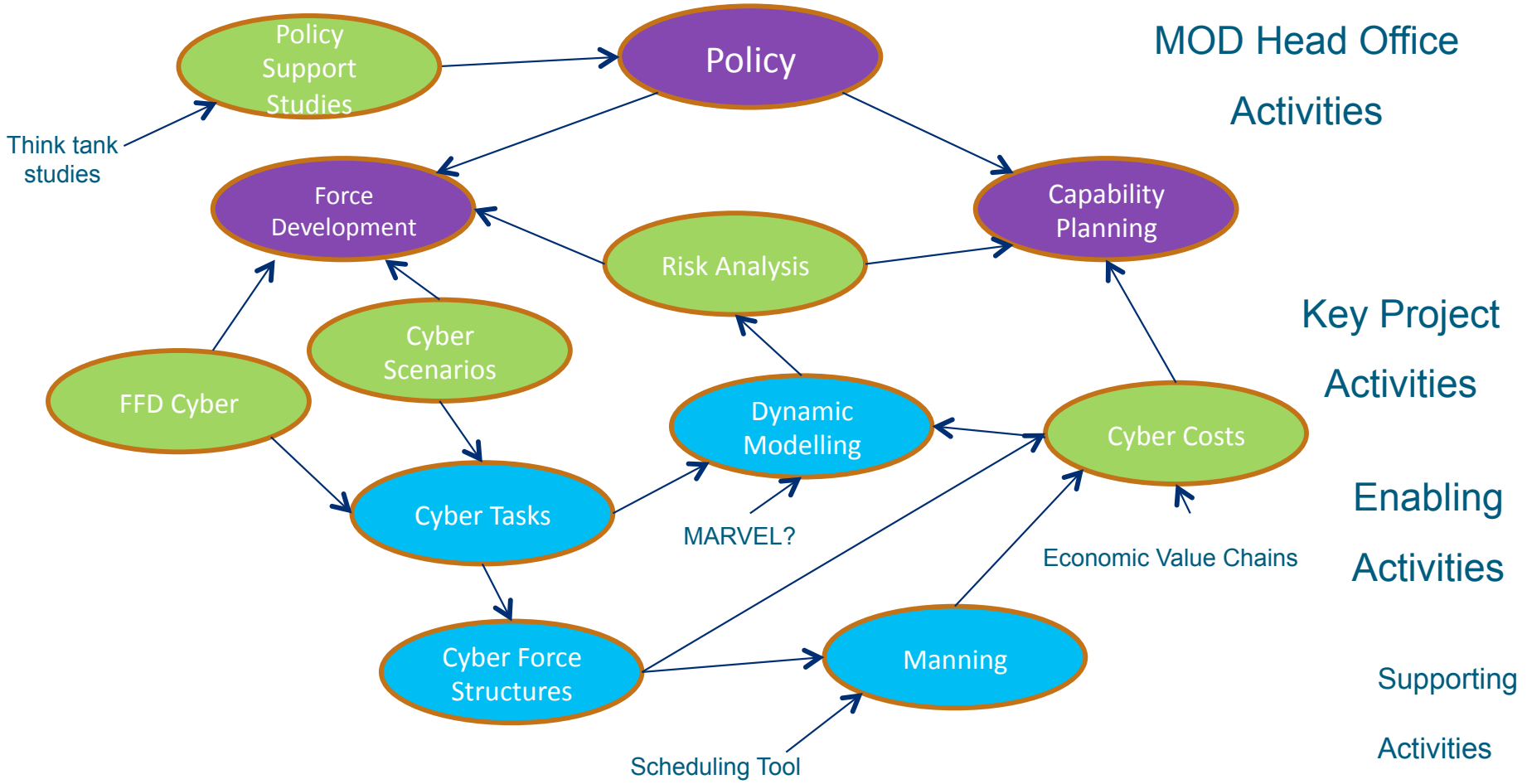
Costs

- Investigate different cyber force elements (FEs) and their associated cost drivers.
- But Cyber Defence is more than just a distinct FE:
  - Includes DCOG but also implicit within other FEs and organisations across MOD;
  - Includes other government organisations outside MOD;
  - Includes industry;
  - Where to draw boundary?

Costs

- Investment in Cyber Defence can *save* MOD money.
- If an opponent disrupts our systems it costs us time and money.
  - Where would such costs be serious?
  - Would investment in improved Cyber Defence help?
    - Economic Value Chains

Cyber Policy & HLOA



Cyber – a Risky Business

- Cyber Defence will never be perfect;
- MOD will always have some vulnerability to Cyber attack.
- Investment in Cyber is a risk-based decision;
- Needs risk-based analysis:
  - Informed by policy, force structures, costs, manning, etc.
  - Need to understand MOD's risk appetite.

Questions

August 2013

Ministry of Defence