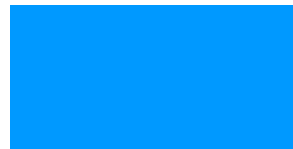
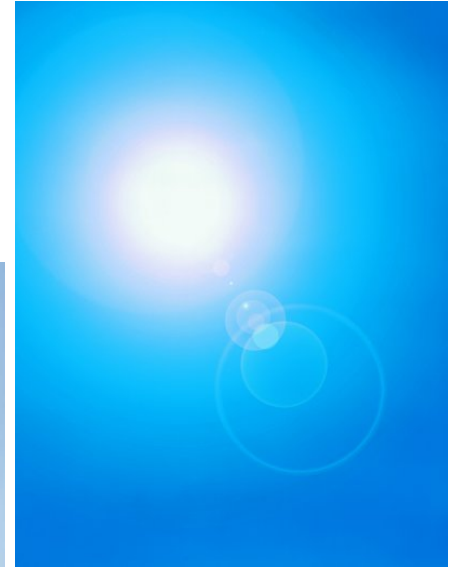


12th ICCRTS, June 2007

Applying a Generic Security Model to the Information Operations Planning Process



Study Objective

Overall Programme

To produce a set of help files suitable for use by new Information Operations staff in the field, files to include both explanatory text and template planning forms and aids

To carry out supplementary studies to inform the generation of help file texts and tools

Work procured by Ministry of Defence, DEC/ISTAR on behalf of Ministry of Defence Directorate of Targeting and Information Operations

Task Objectives

1. To assess the suitability of a generic security risk assessment model for re-engineering into an information operations planning tool
2. If found suitable, to express that re-engineered model as help-file texts for use in theatre by Information Operations staff – *in the context of identifying desired effects and then selecting appropriate weapons (kinetic or non-kinetic) to achieve those effects*

A Caveat:

Study hypothesis is that the generic model will prove suitable. This will only be demonstrated by experience; the study's objective is simply to produce a plausible, testable candidate approach.

Some (UK MoD) Definitions

Information Operations

Co-ordinated actions undertaken to influence an adversary or potential adversary in support of political and military objectives by undermining his will, cohesion and decision-making ability, through affecting his information, information-based processes and systems while protecting one's own decision-makers and decision-making processes.

Effects-Based Approach

The way of thinking and specific processes that, together; enable both the integration and effectiveness of the military contribution within a CA (Comprehensive Approach) and the realisation of strategic outcomes

Effects

Changes as a result or consequence of actions, circumstances or other causes

The Generic Security Risk Assessment Model

HMG (UK) Definition of Risk

The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

The risk causal chain is therefore: Threat → Vulnerability → Impact

The generic approach is:

- Identify and value your assets
- Identify the threats to your assets
- Identify your assets' vulnerabilities – and its counter-measures
- Identify the consequences of asset compromise (the impact)
- Assess the risks for significance to the organisation

The Generic Security Risk Assessment Model - Translated

Security

Impact

Asset

Asset owner

Threat

Vulnerability

Counter-measures

Information Operations

Effect

Target

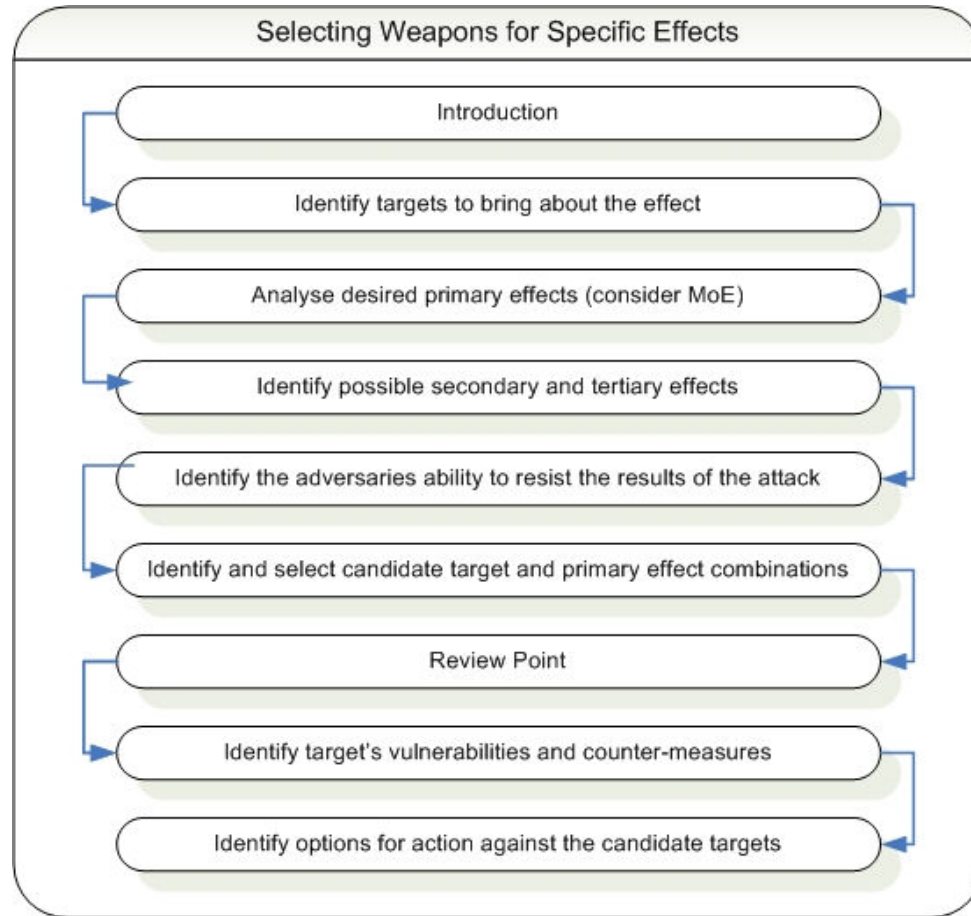
Adversary

Us

Vulnerability

Target defences

The Re-Engineered Model



Current Work

In Progress

- Further exploration of risk models for use in assessing likely adversary courses of action
- Inclusion of adversary courses of action assessment methods in help file texts
- Scenario-based workshop assessments of help file effectiveness
- Adversary team characteristics and vulnerabilities

Future Work

What I would *like* to do next...

- Explore Measures of Effectiveness in this context, and see whether security and other established risk quantifications have anything to offer
- Explore the overlap between risk models in this context, and risk models in the context of Operational Security, Force Protection and assessment of home-side vulnerabilities to adversary information operations
- Explore the possibilities afforded by modern visualisation techniques to produce information operations overlays for intelligence preparation of the battlespace
- Assess whether the use of a risk model offers any possibilities for re-expressing and re-focusing the Request For Intelligence process
- Look at things in reverse – do the disciplines of military, especially information operations, planning, offer insights which can be reflected back into the traditional security domain?

Contact Details

Michael E J Stubbings

QinetiQ

Woodward Building

Malvern Technology Centre

St Andrews Road

Malvern

Worcestershire

WR14 3PS

UK

mstubbings@qinetiq.com

Tel: +44 (0)1684 895845

Fax: +44 (0)1684 896660