12th ICCRTS

"Adapting C2 to the 21st Century"

Applying a Generic Security Risk Model to the Information Operations Planning Process

Topics: Information Operations; Risk Assessment; Effects-Based Planning

Author: Michael E J Stubbings
Point of Contact: Michael E J Stubbings

QinetiQ
Room B007, Woodward Building,
Malvern Technology Centre
St Andrews Road
Malvern
Worcestershire
WR14 3PS
United Kingdom

Tel: +44 (0) 1684 895845

Email: mstubbings@qinetiq.com

Abstract

This paper describes work done in response to a commission from the Ministry of Defence DEC ISTAR office, on behalf of the MoD Directorate of Targeting and Information Operations. The overall requirement was to provide guidance to Information Operations staff both in the UK and in theatre. The objectives of the particular work package discussed in this paper were:

- to assess the suitability of a generic security risk assessment model for re-engineering into an information operations planning tool;
- if found suitable, to express that re-engineered model as help-file texts for use in theatre by Information Operations staff.

This paper describes the results of that work package. A causal risk chain of the form threat→vulnerability→impact was re-engineered into a set of operational planning procedures, expressed in terms of effects-based operations. These procedures were expressed as help-file texts in a prototype tool which MoD is now evaluating for use by Information Operations planners. The paper explains the reasoning behind this re-engineering, and the paper's appendix consists of relevant extracts from the tool's help-file texts.

Outline of Paper

The paper establishes the hypothesis that the generic security risk model can be re-engineered for Information Operations planning purposes. In effect, this means that instead of thinking of oneself as the asset owner (the person with something to lose if a risk is realised) one uses the risk model by taking the stance of the threat. The asset owner is therefore the adversary – thus reversing the normal way the model is used. The model is described, along with the customary way of using it in the information security profession. The reverse engineering of that model and its usage are then described, and formulated as a structured progression for an Information Operations planner from receipt of a Commander's Intent, through to the production of an Information Operations plan. Established security risk properties are re-expressed as target or effect properties to assist in plan construction and evaluation.

The paper itself shows the reasoning behind this reverse engineering. The appendix shows the results: relevant extracts from the help file texts which are now being evaluated by UK Information Operations staff at Permanent Joint Headquarters and in theatre.

Work on this topic continues as the MoD customer, having considered the results described in this paper, has asked for a similar mapping of the generic risk model to be done to assist Information Operations staff to evaluate potential adversary courses of action in the Information Operations domain.