12th INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM

Adapting C2 to the 21st Century

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

Author: Michael E J Stubbings

Organisation: QinetiQ

Woodward Building
Malvern Technology Centre
St Andrews Road
Malvern
Worcestershire
WR14 3PS
United Kingdom

Tel: +44 (0)1684 895845
Fax: +44 (0)1684 896660

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.

Definition of Terms

1. The concept of an Effects-Based Approach is described in UK Ministry of Defence doctrine[1]. In that document (paragraph 106) it is defined as:

   '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'

   In the same paragraph effects are defined as:

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

   There are of course other related definitions; related terms are in extensive use in other nations' military planning and doctrine circles. The key point is that this approach encourages planners to focus on the effects they wish to achieve (e.g. a particular change in the adversary's behaviour) rather than on the immediate outcome of a particular action (e.g. the destruction of a particular facility, or the arrest of a particular person).

2. An example of this might be the need to neutralise an adversary's fuel distribution facility. The effect required is that the facility is rendered unavailable to the adversary, with no possibility of restoration during the period of conflict. This could be achieved by total destruction (a goal-orientated approach). If, however, the adversary forces were sufficiently demoralised already, a lesser attack (i.e. a cheaper one) could achieve the same effect by inducing the adversary's forces to flee the facility and not return. This would also reduce the later reconstruction costs – particularly important if one's own forces wish to make later use of the facility.

[1] Development, Concepts and Doctrine Centre, Ministry of Defence (2006), Joint Doctrine Note 7/06 – Incorporating and Extending the UK Military Effects-Based Approach, Shrivenham

3. While the Effects-Based Approach is the context for this study, it was commissioned with Information Operations specifically in mind. This is defined in UK military doctrine[2] (paragraph 201) as:

> *'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.'*

The Hypothesis

4. It has been suggested[3] that the classic generic model of risk assessment could be 'reverse-engineered' to produce a useful model, or at least a conceptual framework, for the planning of Effects-Based Operations. This can be illustrated by the way this model is built into the various tools and techniques associated with information security risk assessment. It is this information security realisation of the model which will be used to explore its suitability for planning Effects-Based Operations.

Aspects of Information Security Risk

Concepts

5. One of the HMG (Her Majesty's Government) security policy documents[4] states in its Glossary that a risk is:

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

6. An information security risk therefore has three components: a *threat* (human or environmental) exploiting a *vulnerability*, thereby causing *harm* (an impact) which one would rather avoid. A fourth entity is implied: an asset. This is some entity (e.g. a particular computer, piece of software, person or business process) which has the vulnerability as one of its properties, and upon which an impact would operate.

7. This causal chain (threat → vulnerability → impact) is simple enough in concept, though in real life matters are more complicated. For example:

   a) A threat may act upon more than one vulnerability (e.g. a hacker may exploit more than one vulnerability in a system configuration);
   b) A vulnerability may, when exploited, cause more than one impact (e.g. a vulnerable employee may, when subverted, compromise more than one business process);
   c) For a particular impact to occur, two or more vulnerabilities may have to be exploited in some manner (e.g. to disable a particular organisation, vulnerabilities in both its primary and disaster recovery sites might have to be uncovered and exploited – or the deliberate compromise of a primary

[2] Development, Concepts and Doctrine Centre, Ministry of Defence (2002), Joint Warfare Publication 3-80 Information Operations, Shrivenham
[3] Suggestion made by Mr Nigel Jones, Business Resilience Capability Leader, QinetiQ Trusted Information Management
[4] Cabinet Office (July 2005), HMG Infosec Standard No 2 – Risk Management and Accreditation of Information Systems, London

site might coincide with the accidental compromise of a recovery site, e.g. because the latter was near an oil refinery which caught fire).

Many-to-many relationships may therefore exist in this causal chain.

8. A further complication is that impacts may themselves cause further impacts. For example, an information system containing a company's customer data may be compromised, and false data entered as part of a criminal attack to defraud both the company and its customer. The initial impact is the theft. Consequent impacts may include:

    a) A civil action by the customer claiming damages in light of a breach of the obligations under the Data Protection Act;
    b) Bad publicity leading to a drop in the company's share price;
    c) Bad publicity leading to other, unaffected, customers taking their business elsewhere;
    d) Interruptions to business while a police investigation takes place;
    e) Interruptions to business while computer forensic investigations take place.

9. There may be some overlap between what is classed as an impact, and what is classed as a vulnerability. If one is a system manager, an impact may be the compromise of a server, or a portion of the network, as it is probably the availability of these which constitute the system manager's day-to-day business objectives. To people managing the business processes depending on that server or network, the unreliability of these is a vulnerability, the impact being delays or compromise of the business processes. It all depends on your point of view.

10. Some care is needed over the scoping of a risk assessment study. The chain of consequences can extend into the far distance in one direction, and the chain of vulnerabilities in the other direction. For example, a vulnerability might be the dependency of an organisation on the mains water supply for air-conditioning and for staff health and hygiene. But what are the exact vulnerabilities which might contribute towards a failure of the water supply? If we are merely a water company customer, it may be sufficient simply to accept the risk of failure and manage it with a compensation regime expressed in a Service Level Agreement rather than investigate further. As far as impacts are concerned, in the theft example quoted earlier one could investigate the impacts consequent upon a drop in share price. The limitations of a risk assessment need therefore to be established with some clarity and some pragmatism.

<u>Processes</u>

11. There exists a range of well-attested methods for assessing information security risk. All of them operate on the following basic model, though the order of actions may vary slightly between methods:

    a) Identify and value the assets to be protected;
    b) Identify the threats to those assets;
    c) Identify the vulnerabilities associated with those assets;
    d) Identify the protective measures already applying to those assets (effectively the complement of the vulnerabilities);
    e) Identify the impacts should the threats act upon the vulnerabilities;
    f) Assemble the assets, threats, vulnerabilities and impacts into risks;

g) Identify the probabilities associated with the risks;
h) Assess the risks for significance to the organisation.

12. Once the risks have been identified and assessed, risk management is undertaken. This is the process of determining one of the following actions for each identified risk:

    a) Accept (i.e. do nothing);
    b) Transfer (e.g. buy an insurance policy);
    c) Avoid (i.e. do not undertake the activity in question);
    d) Mitigate (i.e. take one or more counter-measures which reduce the likelihood or severity of one or more of the threat, vulnerability or impact).

13. This process has been partly automated in risk assessment methods such as CRAMM[5] and COBRA[6]. Individual components such as threat may be assessed using defined methods such as that developed by Dr Andrew Jones[7].

14. A key aspect of any risk management strategy will be cost. This can be expressed in a range of ways. At one end is the financial cost of the selected counter-measures, or the opportunity cost of a risk avoided. At the other end are the financial, reputational and potentially legal costs of the undesired impact.

15. Mitigation efforts can be directed at impacts. The lessening and/or controlling of an unwanted impact can be a realistic response to a risk. Thoughtful risk managers are likely to have those responses prepared well in advance. Examples of such responses are Business Continuity / Disaster Recovery plans, and Incident Response procedures. An example of the former might be the regular off-site storage of backup media, combined with information system resources elsewhere, available within a pre-determined and acceptable time period. An example of the latter might be the procedures to be invoked should a malicious software incident occur, or a crime be suspected.

Application to the Effects-Based Approach

16. To use this model in the Effects-Based Approach, we must turn it round. The concepts and processes set out above are described from the perspective of an asset's guardian or owner. That person is seeking to prevent the risk being realised, and thus prevent the impact from occurring, or at the very least to minimise the harm which occurs. The counter-measures are selected and implemented in order to achieve this.

17. In conducting military operations against some target we are not, however, the asset owner. We are instead the threat. We are seeking to compromise an asset belonging to someone else. We are seeking ways of circumventing the counter-measures in place. We seek to identify and exploit some vulnerability in order to produce the desired effect (the impact). We must therefore seek a sufficient understanding of our own capabilities (defining the threat); the nature of the asset; the vulnerabilities associated with that asset; and the impact we wish to bring about.

---

[5] CCTA Risk Assessment and Management Method – the HMG-originated approach licensed to Insight Consulting of Walton-on-Thames, Surrey
[6] Consultative Objective & Bi-Functional Risk Analysis – marketed by C&A Systems Security Ltd of Macclesfield, Cheshire
[7] http://people.emich.edu/pstephen/E_M_U_files/Cybercrime-1/Threat-Method-Phase-1.pdf, accessed 28th December 2006

18. There are parallels between the customary use of information security risk models and the conduct of military operations. Both exploit tangible entities (e.g. computer systems or weapons platforms) and intangible entities (e.g. data or business processes or military techniques). Security models are designed for use across a range of domains: Physical; Procedural; Personnel; Electronic. The military Effects-Based Approach similarly operates across a range of domains: Physical; Social; Scientific and Technical; Economic; Legal; Political; Military. Desired effects might be realised in any one or more of these domains. Some common elements are clearly to be found between these two sets of domains.

19. Another way of looking at domains is that identified in the NATO C2 Code of Best Practice[8] which notes that measurements of operational effectiveness (impacts/effects) can be made in the Physical, Information and Cognitive domains. The physical domain is an obvious area of overlap between security and military instantiations of the basic risk model. The security consideration of an electronic domain would appear to have much in common with the NATO C2 scientific and technical, and information domains. Traditional information security risk assessment does not generally address the cognitive domain, although the provision of demonstrably good security training might be seen as a personnel or cognitive issue. Consideration of a cognitive domain is perhaps something that the information security profession can learn from military thinking.

20. The same entities (asset, threat, vulnerability, impact) would seem to be involved whether one is the asset owner or the threat. The same causal chain would seem to be involved: threats operating on vulnerabilities to have an impact on an asset.

21. Just as the risk manager will have to decide whether the cost of the impact justifies the cost of the counter-measures to prevent or manage it, so the planner or the relevant commander will have to weigh up the advantages gained by the desired effect, balanced by the cost of the actions necessary to achieve that effect.

22. The risk manager will also consider the potential reactions to a realised risk and its associated impact. Disaster recovery plans and incident response plans were mentioned above as a frequent information security response to impact management. The planner of Effects-Based Operations will also consider the potential reactions to the desired impact (effect). Will the people associated with the effect be able to react in a way which mitigates or negates the effect? If so, what is the target's end-state likely to be after the mitigation has taken place?

23. In light of these similarities, do the broadly-accepted information security risk assessment concepts therefore offer us a model for researching and planning an effects-based activity? That is the question addressed by this paper.

A Significant Caveat

24. There is one issue which needs open acknowledgement if the relationship between information security risk assessment and effects-based operations

[8] CCRP, (2002), Department of Defense Command and Control Research Program, NATO Code of Best Practice, Washington DC, ISBN 1-893723-09-7

planning is to be explored. It is in essence the difference between linear and non-linear modes of thinking.

25. The causal chain presented at the beginning of this paper is linear. That is the way information security specialists approach risk. We define the threat, the vulnerabilities and the impact we wish to avoid or mitigate, and we define counter-measures to achieve our objective. Simplistically, it could be said that at that point the job is done: the risk is managed. This linear mode of thinking – the single line of thought with a defined beginning and a defined end – has evolved somewhat. It is standard practice to recommend that organisations revisit their risk assessments periodically, and at certain key points (e.g. after a security incident, or when revising the portfolio of applications resident on a server cluster). This has been further developed in the Plan-Do-Check-Act cycle set out in international standards such as the information security standard, ISO27001.

26. It remains the case, however, that information security risk assessment is about one-dimensional causal chains which are revisited from time to time. Even with the many-to-many possibilities of threat-to-vulnerability, or vulnerability-to-impact, this changes only the complexity of the one-dimensional causal chain. It does not change its dimensionality.

27. There are chains of cause and effect in the battlespace, but these are not the one-dimensional causal chains customarily considered by information security specialists. As Atkinson and Moffat[9] point out, military organisations and the environment in which they operate are Complex Adaptive Systems which do not necessarily act and react in a linear manner. Instead, complex interactions take place across multiple domains with consequences both predictable and unpredictable.

28. This observation need not invalidate the hypothesis at the heart of this paper – at least, it need not do so if the risk assessment model is capable of operating in the context of Complex Adaptive Systems. For the moment, it will be assumed that it can operate in that manner. This assumption must be tested at an early point in any further exploration of this subject.

29. It should, however, be noted that a complementary study to this one might be worthwhile: the application of current Command and Control models (e.g. those associated with the concepts of Complex Adaptive Systems) to classic information security risk assessment. Learning from others is rarely a one-way process.

Observations About Tools for Planning Effects-Based Operations

30. An Internet search on the various combinations of ‘planning’, ‘Effects-Based Operations’ ‘Effects-Based Approach’ and ‘planning tool’ shows that a considerable amount of work has been done, and continues to be done. The search outcome demonstrates that much of the thinking about these issues is orientated around one particular area: the contribution made by combinations of ‘effects’ to broader ‘objectives’ which are compliant with, and contribute towards, the Commander’s Intent. Tools and techniques currently under development present these relationships in the context of broader situational awareness approaches.

[9] CCRP (July 2005), Department of Defense Command and Control Research Program, The Agile Organization

31. The ‘upward’ and ‘sideways’ relationships of an ‘effect’ (with the Commander’s Intent and with other effects) are thus being considered. There is also some exploration of the matching of particular resources (e.g. kinetic or non-lethal) to the effect required. A key aim of these developments is the efficient and effective sharing of information (especially situational awareness) across the various participants in a joint command or other collaborative organisation.

32. The concepts involved in the various elements of Effects-Based Operations (aims, effects, actions etc.) are also being explored, and work is being done in both the UK and the US to consider lexicons.

33. These various studies have greatly expanded thinking on how to bring together the information needed by a planner of Effects-Based Operations, and make that information visible and comprehensible. They have also expanded our understanding of how ‘effects’ relate to broader military and political objectives and to the Commander’s Intent.

34. Planners have of course been making plans throughout military history. One difference now is the explosion in information available to the planner, both in terms of quantity and in terms of rate of change – battlespace situation changes can be reflected in near real time on the workstation of a military planner. Another difference is that military organisations are now likely to be operating in parallel with other bodies, including coalition, civil, political, international and humanitarian groups. These organisations, their agendas, objectives, capabilities and constraints have made the military planner’s role even more multi-dimensional than it was before. That is before one factors in the continuously increasing complexity of modern weapons systems, platforms and deployment possibilities.

35. In light of this explosion in complexity, it is not surprising that work has also been done on the mental constructs and processes involved in producing a viable effects-based plan. It is that ‘low level’ aspect which this paper considers: how to get from a desired effect to a plan to achieve that effect.

36. So, does the risk assessment model presented earlier provide a generic structure for determining a plan for achieving a desired effect? In the absence of a pre-existing generic structure with which the risk assessment model can be compared, this question can only be answered by re-engineering the risk assessment model, and see if is at least plausible in its new role.

A High-Level Model For the Effects-Based Approach

Some Initial Points

37. This model is based on two provisional assumptions:

    - The planner knows what effects are required in order to comply with the Commanders’ Intent. There is no requirement for the model to help the planner identify what those effects should be;
    - The generic risk assessment model presented earlier in this paper (paragraph 13) is valid for planning using the Effects-Based Approach.

38. The first assumption above does not imply that the risk model is inappropriate for determining candidate effects to match a Commander’s Intent, or for testing

candidate effect portfolios. The model may perhaps have some role of that sort to play, but that possibility remains to be explored.

39. The remainder of this section of the paper takes the concepts set out in paragraph 13 and re-orders and re-expresses them in a form relevant to planning in the context of the Effects-Based Approach, particularly in the area described as Information Operations (the context in which this work was commissioned).

Identification of Impacts (Asset Compromises)

40. The input to this stage is the effect or set of effects required in order to fulfil the Commander's Intent. The output would be the set of compromises of adversary assets required to achieve the effect.

41. This stage is analogous to the information security risk assessment stages 'Identify and value the assets to be protected', and 'Identify the impacts should the threats act upon the vulnerabilities'. The latter stage is, for risk assessments, relatively late in the process, as one is projecting 'forward' to the impact from the known threats and vulnerabilities. In the case of effects-based military planning, we are working 'backward' from the known (i.e. desired) impact to the threat and vulnerability combination required to achieve that impact. One always starts with what one knows, so impact identification must of necessity be earlier in the process for military planning than for security risk assessment.

42. The aim of this stage is to identify which adversary assets must be compromised in order to achieve the effect, and to establish the characteristics of that compromise (e.g. total destruction of facility, denial of use of a facility for 1 week, loss of civilian support to local military or political establishment). A further dimension to those characteristics is the identification of secondary (direct) effects and tertiary (indirect) effects from the primary (intended) effect, together with an assessment of each one as wanted, unwanted or neutral. It is quite possible that the effect one actually wants is in the secondary or tertiary categories; the primary effect (the direct consequence of a proposed action) may simply be the means to an end. The terms Primary, Secondary and Tertiary should therefore not be considered as indicating relative priorities.

43. It is interesting to note that the military convention of primary, secondary and tertiary effects does not have an analogue in the information security generic risk models. The acquisition of a structured understanding of cascaded effects is an area where information security risk assessors might well have something to learn from military insights.

44. In parallel with the determination of compromise characteristics, the planner should also consider the criteria by which success or otherwise would be assessed should an attack be mounted, together with the means by which the raw data on attack results would be obtained. The subject area here is Measures of Effectiveness, extensively explored in much current thinking about military planning[10]. Some work has been done on the subject of information security valuation systems[11] (see also the references in that paper), and this is another

[10] CCRP, (2002), Department of Defense Command and Control Research Program, NATO Code of Best Practice, Washington DC, ISBN 1-893723-09-7

[11] Stubbings, QinetiQ, (2005), Paper presented to 2005 International Command and Control Research and Technology Symposium, Information Security Valuations: Definitions, Structure and Properties, http://www.dodccrp.org/events/2005/10th_ICCRTS/CD/papers/088.pdf (accessed 28th December 2006)

area where military thinking may have useful lessons which the information security world could take forward.

Identification of Assets

45. At this point the planner identifies those assets which must be compromised in some way so as to achieve the desired effect. Military actions might be aimed at achieving effects in any of the following areas:

    - Physical;
    - Social;
    - Scientific and Technical;
    - Economic;
    - Legal;
    - Political;
    - Military.

    An initial approach to identifying effects might be to consider candidate assets in each of the above domains in turn.

46. It was noted above that the terms Primary, Secondary and Tertiary when applied to effects do not necessarily indicate relative priorities, as the desired effect may be a consequence of some potential action rather than a direct result of that action. When identifying candidate target assets one should therefore keep in mind this possibility: the effect one wishes to achieve may not be directly related to the asset one wishes to compromise. For example, the way to achieve a particular change in attitude in a civilian population may not involve any action directed at the population concerned (e.g. not a leaflet drop or other element of psychological operations) but by arresting some well-known person – given that the proper legalities are observed. The primary effect (taking that person out of circulation) may be desirable, but the desired effect is actually the tertiary (indirect) effect brought about by the 'message' that the arrest sends to the local population.

Identification of Compromises

47. An information security specialist will generally consider asset compromises under the headings of confidentiality, integrity and availability. There are parallels between desired military effects and these categories of compromise. For example, denying the use of a facility to an adversary is a compromise of that facility's availability. An information operation to decrease a population's trust in an information source such as a state television station is effectively an operation against that station's integrity. But military planning has long used its own categories of compromise: degrade; deny; damage; destroy. It is not immediately apparent that the traditional information security vocabulary offers advantages over that already in use for military planning. The application of Confidentiality, Integrity and Availability ('CIA') concepts might however merit exploration at some point.

48. For each intended compromise, whatever vocabulary is adopted, the characteristics of that compromise must be identified. The following headings indicate some candidates for such characteristics.

    a) Permanence (e.g. whether a facility might be repairable);
    b) Duration (e.g. for how long should a facility be unavailable);

c) Time constraints (e.g. the period in which a compromise must take place to have maximum, or at least the desired, effect);
d) Degree (e.g. cause a population to experience discontent, or cause a population to riot or overturn local government).

49. For each asset/compromise combination, a justification should be given as to how this compromise would fulfil the Commander's Intent, and achieve the desired effect.

50. Having identified these characteristics, the planner should also identify the information which would be required after an attack to assess the attack's level of success. This information has to be gathered somehow, and means for doing so will have to be identified, although not necessarily at this point. A further requirement is the identification of a criterion (or criteria) by which success or otherwise can be assessed. This can be considered at two levels: that of achieving the overall desired effect; and achieving the asset compromise meant to bring about the desired effect. It is quite possible that the latter might show a successful attack, but the desired effect never comes about because of some unsuspected factor, or because the significance of the asset concerned was over-rated. It should be remembered that failure sometimes happens – but the first step to mitigating failure is to recognise when it happens. So the 'success or otherwise' assessment criteria must include the 'otherwise'. If we do succeed, how will we know? If we do fail, how will we know? We need to answer both questions. These criteria are not necessarily going to be binary in nature; we must try to find out the *extent* to which we have succeeded or failed.

Identification of Consequences

51. We now have a set of assets and intended compromises of those assets. Each compromise must now be assessed to consider what the knock-on effects might be: the secondary (direct) and tertiary (indirect) effects. For example, denying the adversary the use of a fuel distribution depot might not only inhibit the mobility of local militias, but if the same depot also supplied domestic fuel to the local population, there could also be significant civilian consequences. If in winter, there could be interruptions to domestic heating, but also to fuel supplies for small local bakeries, for example, denying the population their bread. These are secondary effects. A tertiary effect might be the reinforcement of the population's support for local militias.

52. It is, of course, not only an adversary or other target who might be affected by our actions. Secondary and tertiary effects can occur in other populations or systems as well. For example, our actions this afternoon will be replayed across the world on CNN tonight. The behaviour and attitude of friendly governments and populations (including our own), of potentially or actually antagonistic governments and populations, or of neutrals might all be shaped for better or for worse by our actions and, importantly, by the manner of their reporting and presentation. The level of co-operation achieved from coalition partners might be affected, again, for better or for worse. It is essential that these consequences be identified, or at least that best endeavours be made to identify them.

53. Each identified consequence should be categorised as one of:

- Desirable;
- Undesirable;
- Neutral.

54. Combinations of asset compromises should also be considered. If several assets have to be compromised to achieve the desired effects, there might be knock-on effects from combinations of compromise which would not result from just one of the compromises on its own.

55. As with the identification of assets, the identification of consequences can be considered under the following headings:

    - Physical;
    - Social;
    - Scientific and Technical;
    - Economic;
    - Legal;
    - Political;
    - Military.

56. It was noted earlier (paragraph 12) that a security risk assessment needs to be bounded if it is to be realistically managed. One could go on ad infinitum chasing consequent effects. The same is true in military planning. The combinations of assets and compromises could be assessed, followed by their consequences, and the consequences of the consequences, and so on. It is a matter of judgement when the stopping point has come. Fluttering butterfly wings may cause hurricanes (or so we are told) but military planning with that degree of detail is unlikely to be cost effective.

57. A key assessment to be made at this point is the likelihood of each consequence, given the execution of the primary compromise. This could be expressed in a number of ways, but a coarse granularity of Low, Medium, High might well prove to be sufficient. It is quite likely that consequences will depend on some other independent factor. For example, a desired effect might be the reduction in a population's support for their government. The population's reactions to an operation revealing details of that government's more shady activities might depend on whether or not a particularly charismatic politician visits the area immediately after the revelations. Where such independent factors can be identified, these should be noted.

58. Prediction is only accurate in retrospect – a nonsense in semantic terms, but a cautionary phrase nevertheless. There will be other consequences too: unpredicted ones and unpredictable ones; ones which perhaps should or could have been foreseen and ones which could not have been foreseen. The approach set out in this paper is not a means for telling the future. Unpredicted effects will occur; predicted effects will fail to occur. Military experience, imagination, information, skill and luck will raise the predictive 'hit rate'. This method seeks to do no more than provide a structure for capitalising on that experience, imagination, information and skill.

<u>Potential Mitigation of Compromises</u>

59. Short of total obliteration, the adversary is likely to have some opportunity to mitigate the effects of the compromises inflicted upon them. The loss of a fuel depot might be mitigated by transferring responsibilities to other fuel depots further away. The collateral damage caused by a city centre air strike might by mitigated by the prompt attention of the local fire brigade. The removal of government propaganda on local television stations (e.g. by destroying

transmitters) might be mitigated by that government and the population having access to satellite broadcast and reception facilities. The effectiveness of the target's opportunities to mitigate the compromises we inflict might well affect how we choose to go about our planning. It is at this stage that this factor should be considered.

60. For each projected asset compromise, the target's mitigation opportunities should be considered. These may of course not be known with any degree of certainty. If this is the case, this should be stated with clarity. For 'unwanted' compromises, the assessment will have to be made as to whether the target's mitigation capability is sufficient to address the undesirability of the compromise in question; in effect, can the target do our work for us by managing sufficiently the unwanted consequences of our actions. In physical terms, this may well be the case. In terms of factors such as the state of mind of the population, this is less likely.

<u>The Asset-Compromise Options</u>

61. We now have:

    a) A list of assets;
    b) Candidate compromises to inflict on those assets;
    c) A description of the relevance of the asset-compromise combination to the desired effect and to the Commander's Intent;
    d) Candidate measures of effectiveness for attacks on the assets in question;
    e) Assessments of secondary and tertiary effects of those compromises;
    f) Categorisation of secondary and tertiary effects into Desirable, Undesirable and Neutral;
    g) Assessments of the probability of those compromises, along with any independent factors which might qualify those effects;
    h) Assessments of the mitigation opportunities available to the target in respect of the proposed primary, secondary and tertiary effects.

62. There might well at this point be a set of alternative approaches emerging. More than one pattern of asset compromise might appear to deliver the intended effect. Each emerging pattern should be described separately. The dependency chain of the secondary and tertiary effects should be identified, possibly in some form of tree diagram – this could form a key communication medium between planners and between planners and commanders.

63. An initial view of the acceptability of the proposed compromises should now be emerging. Discussions with commanders may rank the alternatives, or even identify some as unacceptable, before planners get to the stage of mapping resources to the proposed compromises. The structured approach to identifying secondary and tertiary effects and the adversary's ability to mitigate those effects will offer some initial opportunity to rank any proposed alternatives.

64. It is also at this point that planners and commanders will identify which of the undesirable consequences need action to mitigate or neutralise their effects if action is taken to bring about the primary effect. This will effectively refine the requirements levied on the plan, and therefore on the planners.

65. It is important that nothing be thrown away at this point. It could be that preferred options, once assessed for their practicability and cost, are shown to be unacceptable. A previously unacceptable combination of assets and

compromises may then become the preferred route to achieving the desired effect.

Asset Vulnerabilities

66. It is now necessary to identify those properties of the target asset which present opportunities to inflict the desired compromise. The base model for information security risk assessment, the starting point for this paper, has an early vulnerability assessment phase. In information security circles it is common to treat vulnerabilities as separate from the threats which might exploit them – indeed, vulnerability assessment of IT systems is often a separate technical discipline employing techniques such as penetration testing.

67. But that is not how the hacker will operate – and it is the hacker who is our analogue in this situation. Hackers will seek out vulnerabilities they know how to exploit, and for which they have the necessary resources. If the hacker does not find a vulnerability matching his knowledge and resources, he or she may well consider searching for other vulnerabilities and amending their own knowledge and resources in order to exploit those other vulnerabilities.

68. The military planner could ask this question: 'What vulnerabilities does this asset have which, if exploited, would compromise it in this way?' Using the example of the hacker, the planner would ask that initial question, but would then also ask: 'What vulnerabilities does this asset have for which I have matching resources capable of exploiting them?' If the answer to this second question is 'none', or 'not enough' then one at least of the following actions must be undertaken:

    a) Further or more appropriate resources must be obtained or tailored to match the known vulnerabilities;
    b) A possibly more detailed reassessment of the target asset must be undertaken to identify other exploitable vulnerabilities;
    c) The projected asset-compromise is abandoned, with possibly an alternative asset-compromise being selected instead.

69. As noted earlier, security counter-measures are the complement of vulnerabilities. Any assessment of a candidate target asset's vulnerabilities must inevitably include an assessment of the asset's counter-measures (protective defences etc.) which mitigate the vulnerability. This stage will inevitably involve consideration of the candidate resources for attacking the adversary asset. For example, an asset might be vulnerable to air or ground attack. It might have both anti-aircraft and ground defences, but the nature and potency of each might be different.

70. The outcome of this stage of the planning process will be:

    a) For each selected asset-compromise combination, a statement of the perceived vulnerabilities associated with that asset;
    b) For each identified vulnerability, an assessment of the counter-measures the adversary has in place to deter or defend against an attack;
    c) For each identified vulnerability, an assessment of the resources required successfully to exploit it, bearing in mind the asset's counter-measures (i.e. defences).

71. It should be noted that a vulnerability might exist in any of the conventional military planning domains: Physical, Information and Cognitive. For example, a

fuel dump might be vulnerable to air attack (physical); information available to an adversary commander might be vulnerable to compromise through a deception operation (information); a target population might be vulnerable to being persuaded not to support a local militia (cognitive).

72. It is at this point that the parallels to the generic information security risk assessment process are complete. We now have our candidate causal chains, leading from the threat (us), through the adversary's vulnerabilities, to a compromise of the adversary's assets, causing a 'business impact' – the effect which we wish to bring about. We have assessed the adversary's counter-measures (the complement of his vulnerabilities) and also assessed the adversary's ability to mitigate the results of a successful attack. In addition, the knock-on effects (secondary and tertiary effects) have been considered, and potential Measures of Effectiveness identified for post-mission assessment.

Selection for Engagement Plans

73. We now have what is in effect a requirements specification for a military activity, set out in terms of:

    a) The target asset;
    b) The desired effect;
    c) The way in which the asset must be compromised to achieve the effect, including the characteristics of that compromise;
    d) Secondary and tertiary effects, together with their desirability, probability, and the ability of the adversary to mitigate the range of effects;
    e) Assessment of the adversary's ability to mitigate the effects of a successful attack;
    f) Ways of measuring the effectiveness of an attack on the target asset;
    g) Exploitable vulnerabilities which would compromise the target asset;
    h) Assessment of the adversary's counter-measures to its vulnerabilities;
    i) Candidate resources for exploiting the identified vulnerabilities.

74. It is quite likely that a set of alternative specifications will now exist, showing different combinations of asset, compromise and vulnerability/resource matching which would achieve the desired effect. Some discussion between planners and commanders might take place at this point to rank the alternatives and identify immediately any which are unacceptable.

75. But there will inevitably be uncertainty. As noted earlier, Complex Adaptive Systems are involved – both ours and those of the adversary or target. All situations existing at the start of the planning process will have changed to some extent by the time this stage of the process has been reached. Two questions then occur: 'which, if any, of these changes are relevant?' and 'in what way are they relevant'. There is no easy answer to this conundrum. In fact, there may not be any 'answer' at all, easy or not. It could be that one simply has to be aware of this, look for it, and cope with it. Coping strategies are likely to include:

    - Continuous, or at least reasonably frequent, re-verification of assessments used in the planning process;
    - Clear identification of assumptions, verifying those which can be verified;
    - Identification of key points of situation volatility (in relation to the target and to ourselves) for frequent checking – given that

constant rechecking of an entire plan is likely to be prohibitively expensive, detrimental to operational tempo and of limited value.

76. A further aspect of uncertainty is that some things we would like to know we simply do not know. We may have no idea at all about the capability of the local fire brigade to handle collateral damage after a city centre air strike. We may have no idea about the dependency of a local population on domestic fuel from a fuel storage depot we wish to neutralise. We may have no idea about the state of mind of a target population and their likely reaction to a snatch operation against a local warlord – or whether that warlord's militia will vent its fury on the local population. Uncertainty is a fact of life. The key point is that it should be, as far as is possible, bounded. To allude to a well-known US defence statement: we should do our best to limit the number of unknown unknowns, replacing them with known unknowns. And if known, they are therefore to some extend bounded and understood.

77. It is at this point that candidate engagement plans can be drawn up, to whatever level of detail is required by the commander.

After The Plan Has Been Written

78. The generic information security risk assessment model presented early in this paper might have something further to contribute to this process. The normal review processes will of course apply, but any military operation carries risks. The generic model could form a basis for carrying out an independent study of an engagement plan to assess the risks associated with that plan. In this case, 'ours' and 'theirs' once again reverse position. It is risk to 'our' assets which becomes the pertinent question, and 'they' become the threat. So, the assets would be our own resources, the impact (or effect) would be damage done to our resources and our mission. The vulnerabilities would be those associated with our resources and procedures, and the counter-measures would be the steps we take to address those vulnerabilities. The target's counter-measures become the means by which our assets might be compromised.

79. Some of the work for such a risk assessment will probably have been done already. For example, secondary and tertiary impacts on friendly and neutral organisations form part of the impacts associated with a mission, and therefore part of the risk carried by that mission. A target's counter-measures will already have been considered as part of the planning process, and those counter-measures form an already identified attack vector.

80. This availability of risk-related information does carry with it the danger that a risk assessment of a plan suffers from whatever limitations may have applied to the original plan, inheriting any unjustified or unrecognised assumptions which may have gone into its gestation. So some degree of independence and constructive scepticism would seem advisable.

81. This subject (the use of the generic information security risk assessment model for plan verification) is not the primary subject of this paper and will not be pursued further at this point. It should, however, be considered for future study.

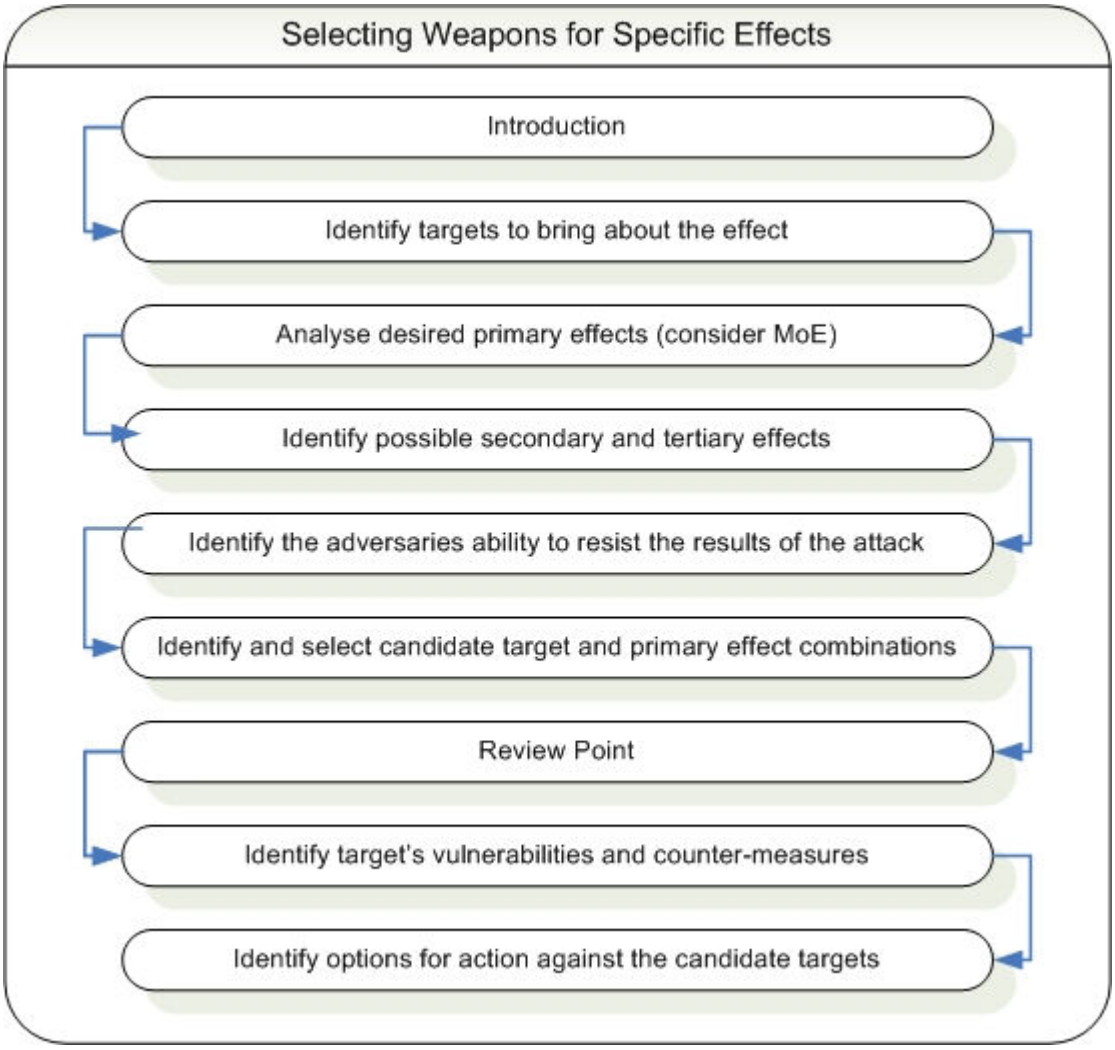
Providing Support To Planners In The Field

82. The work done to prepare this paper formed part of a much larger activity commissioned by the UK Ministry of Defence, on behalf of its Directorate of

Targeting and Information Operations (DTIO). The aim was to produce a set of help-texts, usable on field-based laptop computers. These texts are intended for new Information Operations officers posted into headquarters roles in the UK and in theatre. The texts are extensively hyper-linked, and include template planning documents to assist Information Operations planners. An initial version of the product (which goes under the name Milipedia) has undergone testing in theatre and the results of that testing are now being reviewed.

83. The material in this paper was rendered into help-text form in the Milipedia section 'How to Select Weapons to Create Specific Effects'. This material, with the permission of the Ministry of Defence, has been attached as an appendix to this paper.

84. Milipedia is being developed further on behalf of DTIO. Current work includes guidance on influencing adversary teams, and the further development of the risk model described in this paper to form an approach to assessing likely adversary courses of action. Other developments are being considered, such as the inclusion of case histories and theatre-specific reference files. The means of delivery are also being considered, with network deployment being a possibility.



Introduction to selecting weapons to create specific effects

So, you know what effects your Commander wishes to bring about. We have to work out ways of implementing the Commander's wishes. Military planners have been doing this for millennia – you are likely to have your own experience, knowledge and insights to bring to this task. This section sets out a framework within which that can be done. It does not replace your contribution, but provides a new structure for it.

The New Structure

The structure is derived from generic approaches to security risk assessment. Risk assessors will generally be acting on behalf of the owner of an asset such as a computer system, a business process, a database or a location. The risk assessor will consider what might happen to compromise that asset, and will seek to put appropriate cost-effective counter-measures in place to protect it. The assessor will look for threats (e.g. hackers, attackers, suborned users, environmental threats such as lighting strike). The assessor will look for vulnerabilities (poorly-managed computer systems, sites without boundary fences etc.) and will match the threats to the vulnerabilities they might exploit. The assessor will also look at the possible consequences (the 'impact') of a risk to an asset being realised.

> The overall risk then is that an identified threat might exploit an identified vulnerability belonging to an identified asset, resulting in an identified impact.

Now turn that around. You are not the asset owner – the asset owner is the opposition. You are the threat. It is your job to make the impact happen – to bring about the effect that the Commander has in mind. The asset is your target. The impact is the primary direct effect. The compromise is your attack. So in military terms we could say:

> The overall risk to the opposition is that you might exploit an identified vulnerability belonging to an identified target, resulting in an identified primary effect.

This procedure takes you through the process of constructing a preferred option for an action against a target. This procedure has the following steps:

- Identifying the targets you need to attack to bring about the Commander's intended effect;
- Analyse desired primary effects on targets;
- Identifying what the secondary and tertiary effects might be;
- Identifying candidate Measures of Effectiveness;
- Identifying what measures the opposition might have in place to mitigate the results of your attack (i.e. to mitigate the effects);
- Identifying and selecting candidate target/primary effect combinations;
- Identifying target's vulnerabilities and counter-measures;
- Identifying options for action against the candidate targets.

Note: Whilst this list is presented in a linear process, elements of your analysis may well be relevant to more than one part of the process at any one time. Remember that this process is not one that is separate from your HQ's targeting process, but is presented in order that you can think about targeting imaginatively and can fully participate in the targeting process.

Identifying the Targets

What targets do you need to attack in order to achieve the desired effects?

Some imaginative flexibility helps here. For example, you may wish to change a civilian population's perception of their local de-facto government. Do you demonstrate the government's ineffectiveness by carrying out a substantial and very visible kinetic attack against an installation? Or do you go for a 'hearts and minds' persuasion operation, using radio transmissions and leaflet drops? Or do you opt for a combination of the two? It could therefore be said that the primary effect of an attack (e.g. against a paramilitary installation) is not actually the object of the exercise. The effect one is really after is a *consequence* of the primary effect.

Any target is likely to exist in one or more of the following seven domains:

- Physical;
- Social;
- Scientific and Technical;
- Economic;
- Legal;
- Political;
- Military.

This checklist is a good starting place for identifying candidate targets, remembering that for any one effect, more than one candidate target may be involved, in one or more of the seven domains.

Even this early in the process, options may be emerging, with distinct sets of alternative targets.

Analysis of desired Primary effects
What do you want to do to the targets you identified in the previous step?

The primary effect should result in a change of state in the target which could be that it is:

Destroyed
Denied
Disrupted
Degraded
Compelled
Convinced
Deterred
Etc.

For each target/effect pair you should now consider the constraints that apply to you. What are your Rules of Engagement? What are you allowed to do – and what are specifically not allowed to do? Some of your rules will be set out in international or UK law. Some will be campaign constraints imposed by senior commanders. Whatever the primary effect, if it is a non-starter because of the constraints which apply to your campaign, it's better to realise that now before too much time is spent on it.

For each candidate primary effect you should now identify the preferred or potential characteristics of that primary effect. Here are some candidate characteristics you might like to consider.

- Permanence (e.g. whether a facility should be repairable or not);
- Duration (e.g. for how long a facility should be unavailable);
- Time constraints (e.g. a window of opportunity presented by external factors such as tides, time of sunrise, validity of a UN mandate, synchronisation with other campaign actions);
- Degree (e.g. induce unrest in a population or incite them to overthrow a government).

It is at this point that you should first consider Measures of Effectiveness. How will you know after the attack whether you have been successful? How will you know whether you have failed? How will you identify and characterise the range of possibilities in between these two extremes? What data will you need to collect during or after the attack in order to establish your Measures of Effectiveness?

Outcome

You should now have:

- A list of permitted targets, possibly grouped into alternative courses of action;
- Descriptions of the proposed primary effects on each target;

- Characteristics of each proposed primary effect;
- Constraints applying to each proposed primary effect;
- Candidate Measures of Effectiveness by which you will eventually assess the effects.

Identification of Consequences

This section is about Primary, Secondary (direct) and Tertiary (indirect) effects. We started with the Commander's desired effects, and noted that what we want to happen may in fact be a secondary or tertiary effect. Our route to that effect may, however, involve some indirection by attacking some separate target.

The question you must ask here is: *If I carry out this attack – what will happen as a result?*

This is an exercise in informed imagination. Prediction is only accurate in hindsight, but we still have to try – otherwise all we ever do is react. The better your information about the target circumstances (e.g. intelligence reports, surveillance imagery, knowledge of the local culture) the more likely you are to predict accurately what the results of your attack will be. You are unlikely to be proved wholly correct.

You may also wish to consider separately potential effects on:

- The opposition (and maybe different categories within the opposition, such as conscript military units versus professional units);
- Our own forces and allies (including civilian populations such as CNN viewers, different effects on different allies);
- Neutrals (potentially neutral states, or neutral actors such as the Red Cross).

From your knowledge of your target environment you may wish to construct your own category checklist. For each primary effect (i.e. the immediate physical or other consequences of your attack) you should consider at least the secondary (direct) and tertiary (indirect) consequences in each of the domains you have decided to consider. Whether you consider further 'consequences of consequences' is up to you, though you are likely to reach rapidly a point of diminishing returns.

You should also consider the effects of combinations of attack. For example, a secondary or tertiary effect may emerge because two particular co-ordinated attacks have taken place rather than taken place at different times.

For each primary, secondary or tertiary effect you have identified, you should also assess the following:

- Is this effect Desirable, Undesirable or Neutral?;
- What is its likelihood (e.g. Low, Medium or High)?

The section entitled 'Planning orders of effects and mitigating against unintended consequences' provides a structure for going through this process.

Outcome

From the previous steps you should have:

- A list of permitted targets, possibly grouped into alternative courses of action;

- Descriptions of the proposed primary effects on each target;
- Characteristics of each proposed primary effects;
- Constraints applying to each proposed attack;
- Candidate Measures of Effectiveness by which you will eventually assess the attack results.

For each target/effect combination you should now have a list of predicted secondary and tertiary effects. For each effect (primary, secondary or tertiary) you should now have:

- Description;
- Likelihood;
- Identity of group(s) subject to the effect;
- Linkages – which primary effect leads to which secondary, which leads to which tertiary (and vice versa – for any one secondary or tertiary effect, which effect causes it);
- Desirability of the effect.

Anticipation of Enemy Reaction to Attack

The enemy will of course be trying to anticipate your attacks and develop counter-measures. We will consider those later. But they are also likely to have measures in place to help them cope with the situation should your attack succeed. These have to be borne in mind by the military planner. They can even work to your advantage. If there are undesirable consequences to a proposed attack, it is possible that the enemy themselves will have measures in place to mitigate those consequences. For example, an attack on transport links might have the desired effect of impeding enemy military supply lines, but with the unwanted effect of denying food supplies to the local civilian population, thus increasing resentment and opposition when the area is finally occupied. The enemy may well have the ability and the will to reinstate the food supplies by other routes, routes which are not suitable for the major military convoys which you will have interrupted.

For each effect (primary, secondary or tertiary) you have identified, you should therefore consider the enemy's likely reaction. That reaction, if it happens, is likely to fall into one of the following three categories for each effect:

- Enhance the power of the effect;
- Diminish the power of the effect;
- Neutral – make no difference.

You may find that as a result you wish to modify the likely chain of consequences from primary effect, to secondary, to tertiary. As well as modifying the effects you have already predicted, the enemy's reaction may bring about an entirely new consequence.

Other modifications to the effect may also occur. For example, the enemy's reaction may include publication to neighbouring countries of details (real or false) of your attack, thus bringing into the sphere of effects other social groups not previously involved.

As noted previously, it is possible to follow the 'consequences of consequences' chain far further than is cost-effective, and it will inevitably be a matter of skill, experience, judgement and the information available as to when to stop following the chain.

It is these same factors which will affect the quality of your prediction of enemy responses. But there is one other factor: luck – both good and bad. You can provide a framework within which to manage the consequences of luck, but you will never eliminate it.

Outcome

From the previous steps you should have:

- A list of permitted targets, possibly grouped into alternative courses of action;
- Descriptions of the proposed effects on each target;
- Characteristics of each proposed effect;
- Constraints applying to each proposed attack;
- Candidate Measures of Effectiveness by which you will eventually assess the attack results.

For each target/effect combination you should have a list of predicted secondary and tertiary effects. For each effect (primary, secondary or tertiary) you should have:

- Description;
- Likelihood;
- Identity of group(s) subject to the effect;
- Linkages – which primary effect leads to which secondary, which leads to which tertiary (and vice versa – for any one secondary or tertiary effect, which effect causes it);
- Desirability of the effect.

To the above list of information about each effect you should now be able to add:

- Likely enemy reaction;
- Your assessment of that reaction – Enhance effect; Diminish effect; Neutral.

You may well also have modified the information you had previously identified for each effect.

First Review Point

You should now have a set of candidate targets, with information about proposed attacks and anticipated consequences. All of these will be derived from a description of the effect desired by the Commander. What remains is to map the capabilities available to you onto these target/attack combinations and then to produce engagement plans.

But before you do that mapping, there is the opportunity now to review the options identified so far and rank them by desirability. This might mean identifying those which have potential consequences which the Commander deems unacceptable.

You can now present the following for review and ranking:

- A list of permitted targets, possibly grouped into alternative courses of action;
- Descriptions of the proposed effects on each target;
- Characteristics of each proposed effect;
- Constraints applying to each proposed attack;

- Candidate Measures of Effectiveness by which you will eventually assess the attack results.

For each target/effect combination you should have a list of predicted secondary and tertiary effects. For each effect (primary, secondary or tertiary) you should have:

- Description;
- Likelihood;
- Identity of group(s) subject to the effect;
- Linkages – which primary effect leads to which secondary, which leads to which tertiary (and vice versa – for any one secondary or tertiary effect, which effect causes it);
- Desirability of the effect;
- Likely enemy reaction;
- Assessment of that reaction (Enhance effect; Diminish effect; Neutral).

The outcome of this review is a ranking of the target/effect combinations, and an indication of what options the Commander finds acceptable or unacceptable.

It is important not to discard any options – even if the Commander does not choose at this point to pursue them. Those rankings may change after the attack practicalities have been considered, and previously unacceptable options may have to be revived.

Assess Target Vulnerabilities

You now have a set of target/effect combinations, probably ranked in order of preference. It is now time to consider the exploitable vulnerabilities of those targets (derived from Target Audience Analysis and Target Systems Analysis). There are two ways of approaching this: Considering what capabilities are available to you, and then looking for vulnerabilities which those capabilities could exploit; or assessing the targets' vulnerabilities independently of whether you can actually do anything about them.

There are dangers associated with both approaches. If you take the 'capability-independent' approach, you could end up wasting time and effort assessing vulnerabilities you are unlikely to be able to exploit. If you take the 'capability-based' approach, you may find your mindset constrained by the resources you have available, and by your customary manner of using those resources. You might then miss some vulnerability which in fact offers you a better chance of attack success.

It comes down to this: know yourself, and recognise the assumptions you are making. Then challenge those assumptions – some will be valid, some may not be. Vulnerabilities might exist in any of the conventional military planning domains: physical; information; and cognitive. These three headings present a useful structure for considering any particular target. Even a desired, apparently physical, effect like disabling an adversary's command network might have vulnerabilities in any of these domains. Installations could be destroyed by kinetic means; false information could be fed into the network; militia units could be induced to defect or flee. Attacks could take effect in one or more of these domains simultaneously, or in some pre-determined sequence. It is not a case of one target to one vulnerability.

You should be asking yourself this question:

> *What vulnerabilities does this target have for which I have matching resources capable of exploiting them sufficiently to cause the desired effect?*

If the answer to the question is 'none', or 'not enough', then you are likely to have to take at least one, possibly more, of the following actions:

- Obtain further or more appropriate resources;
- Tailor existing resources to the task in hand;
- Reassess the target to seek other, more exploitable, vulnerabilities;
- Abandon the relevant target/attack combination as not feasible.

Once you have identified vulnerabilities which you believe exist, and can be exploited, it is necessary to consider whether the enemy has counter-measures in place which will lessen the significance of those vulnerabilities: for example, the extent to which a vulnerability to airstrike is mitigated by a target's collocation with a civilian/ dual use facility.

Outcome

You should now have:

- A list of permitted targets, possibly grouped into alternative courses of action;
- Descriptions of the proposed effects on each target;
- Characteristics of each proposed effect;
- Constraints applying to each proposed attack;
- Candidate Measures of Effectiveness by which you will eventually assess the attack results;
- A ranking to indicate the Commander's preference out of the target/effect options presented.

For each target/effect combination you should have a list of predicted secondary and tertiary effects. For each effect (primary, secondary or tertiary) you should have:

- Description;
- Likelihood;
- Identity of group(s) subject to the effect;
- Linkages – which primary effect leads to which secondary, which leads to which tertiary (and vice versa – for any one secondary or tertiary effect, which effect causes it);
- Desirability of the effect;
- Likely enemy reaction;
- Assessment of that reaction (Enhance effect; Diminish effect; Neutral).

For each target you should now also have a set of vulnerabilities. For each vulnerability you should have:

- Description;
- Assessment of the enemy's matching countermeasures;
- Assessment of the resources required successfully to exploit the vulnerability;
- Initial assessment of the availability and suitability of candidate resources to conduct the attack.

Selection for Action

The outcome from the previous step is a set of alternative specifications for achieving the desired results. In outline each specification will have:

- What we want to achieve (the effect);
- What we want to attack (the target);
- Constraints applying to the attack (e.g. times, sequences);
- The way we want to attack the vulnerabilities;
- The resources we want to carry out the attack.

This information forms the basis for the decision concerning which options to select. Your outline plan can then be used as a template to fill in the details of who must do what: For example, what ordinance is required; what platforms; what manoeuvres by what units; what leaflet drops with what information.

It should be noted that participant groups in the battlespace can be regarded as Complex Adaptive Systems. The implication is that situations will change as these systems interact, whether positively or negatively. The following four questions should therefore be asked.

1. What has changed? (Note here that you should re-verify your assumptions, not simply look for 'observable' changes in the battlespace).

2. Which, if any, of these changes matter?

3. In what way do these changes matter?

4. What, if anything, must I do to respond to these changes?

When should these questions be asked? Probably not continuously otherwise no real planning would ever get done. Probably at certain key points in the planning process, such as immediately before presenting plans for selection and action. Probably after some key change has been observed in the target, the enemy, or when one's own side's circumstances change (e.g. when Rules of Engagement are amended, or a capability is unexpectedly depleted).

Do not expect to know everything. Much will remain unknown until after the engagement, if then. But make sure you differentiate between what you truly know, what you suspect, what you believe and what you assume. These are not the same things, and you should weight them accordingly.

Please note:

This is an extract from Milipedia, which is a series of help files that offers advice and guidance to UK Information Operations planners. Milipedia does not state MOD policy and readers should not infer that any activities mentioned would be conducted by UK or its armed forces.