

The Analysis of Compound Information Warfare Strategies

C. Kopp

Clayton School of Information Technology,
Monash University, Australia
E-mail: carlo@csse.monash.edu.au

Abstract

The practical defensive and offensive application of Information Warfare most frequently involves the use of complicated compound strategies, in which multichannel and multilayered attacks must be analysed. This paper presents a systematic approach to the analysis problem, which is exploitable for defensive and offensive purposes.

Keywords

Deception Techniques, Information Warfare, Strategic Deception, Tactical Deception, Perception Management

INTRODUCTION

Information warfare attacks in practice most frequently involve complicated multilayered and multichannel strategies. Such complex compound strategies arise by players aggregating and combining often a large number of canonical strategies.

All strategies used in information warfare are combinations or forms of the four canonical strategies, each of which involves a specific mode of attack on an information channel or system (Borden, 1999; Kopp, 2000).

The four canonical strategies of Information Warfare can be defined thus (Kopp, 2003):

1. **Degradation or Destruction [also Denial of Information]**, i.e. concealment and camouflage, or stealth; Degradation or Destruction amounts to making the signal sufficiently noise-like, that a receiver cannot discern its presence from that of the noise in the channel.
2. **Corruption [also Deception and Mimicry]**, i.e. the insertion of intentionally misleading information; corruption amounts to mimicking a known signal so well, that a receiver cannot distinguish the phony signal from the real signal.
3. **Denial [also Disruption and Destruction]**, i.e. the insertion of information which produces a dysfunction inside the opponent's system; alternately the outright destruction of the receiver subsystem; Denial via disruption or destruction amounts to injecting so much noise into the channel, that the receiver cannot demodulate the signal.
4. **Denial [also Subversion]**, i.e. insertion of information which triggers a self destructive process in the opponent's target system; Denial via subversion at the simplest level amounts to the diversion of the thread of execution within a Turing machine, which maps on to the functional behaviour of the victim system, i.e. surreptitiously flipping specific bits on the tape, to alter the behaviour of the victim Turing machine.

A problem which frequently arises in practice is that of understanding and analysing a complex compound deception strategy. Given that such a strategy can comprise a very larger number of canonical primitives, properly understanding the structure of the strategy, and thus its underlying aims, can present difficulties.

A good example is a scenario in which an opponent is playing a very complex compound deception strategy. The aim of the defender is to determine whether gathered information is a deception or not, and what the specific aim of that deception might be. In the simplest of terms, 'what does this opponent want me to think and why?'

Detection of inconsistencies, mistakes or gaps in such a complex deception strategy may be the only method of unmasking such a deception, especially if the deception is carefully architected from the outset.

Another problem which can frequently arise is that of countering an opponent's deceptive perception management strategy. Such deceptions can often be complex compound strategies in which multiple mutually

reinforcing falsehoods are employed with a specific aim of shifting the perceptions of a victim audience. Often the only technique for defeating such a strategy is to unmask the deception before the audience. A well crafted compound strategy may present genuine difficulties in analysis.

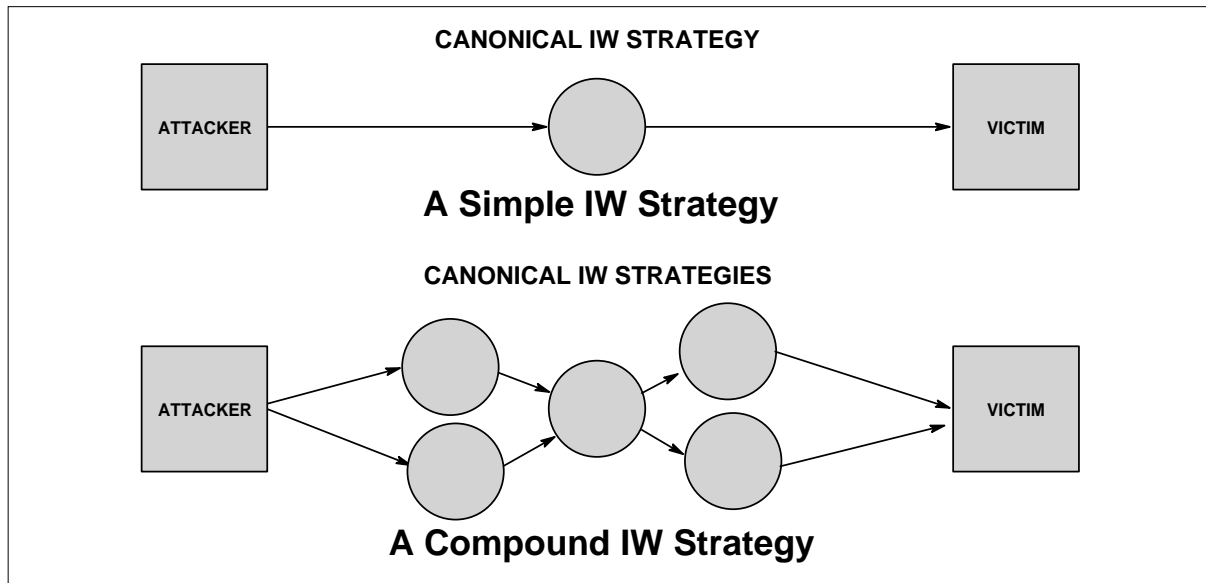


Figure 1: Simple and compound information warfare strategies (Author).

The aim of this paper is to present a systematic method for structural analysis of complex compound information warfare strategies, exploiting the orthogonality properties of the four canonical strategies of information warfare.

PRIMITIVES , PRECEDENCE AND COMPOUND STRATEGIES

To model the structure and behaviour of a compound information warfare strategy, it is necessary to first define the primitives which form the components of the model.

The Attacker:

The attacker is the player in an information warfare strategy who is executing the strategy against a victim player.

The Victim:

The victim is the player in an information warfare strategy who is being subjected to an attack by the attacker.

Canonical Strategy:

A canonical information warfare strategy is defined as one of the four fundamental strategies. These strategies are atomic, in the sense that any compound strategy can be divided into a number of canonical strategies, but a canonical strategy cannot be further divided in any way. Refer Figure 1.

Compound Strategy:

A compound information warfare strategy is any strategy which comprises more than one canonical information warfare strategy, and in which some defined precedence relationship exists between these strategies. Refer Figure 1.

Precedence Relationships:

A precedence relationship defines the order or precedence which exists between more than one canonical information warfare strategy comprising a compound strategy. In practical terms, one canonical strategy can be a precedent to one or more canonical strategies. The precedence relationship cannot be bidirectional since the

time domain is not bidirectional. It is only once the precedent strategy has achieved some effect, that the antecedent strategy can produce its effect. There is no bound on the number of precedent strategies to any antecedent strategy.

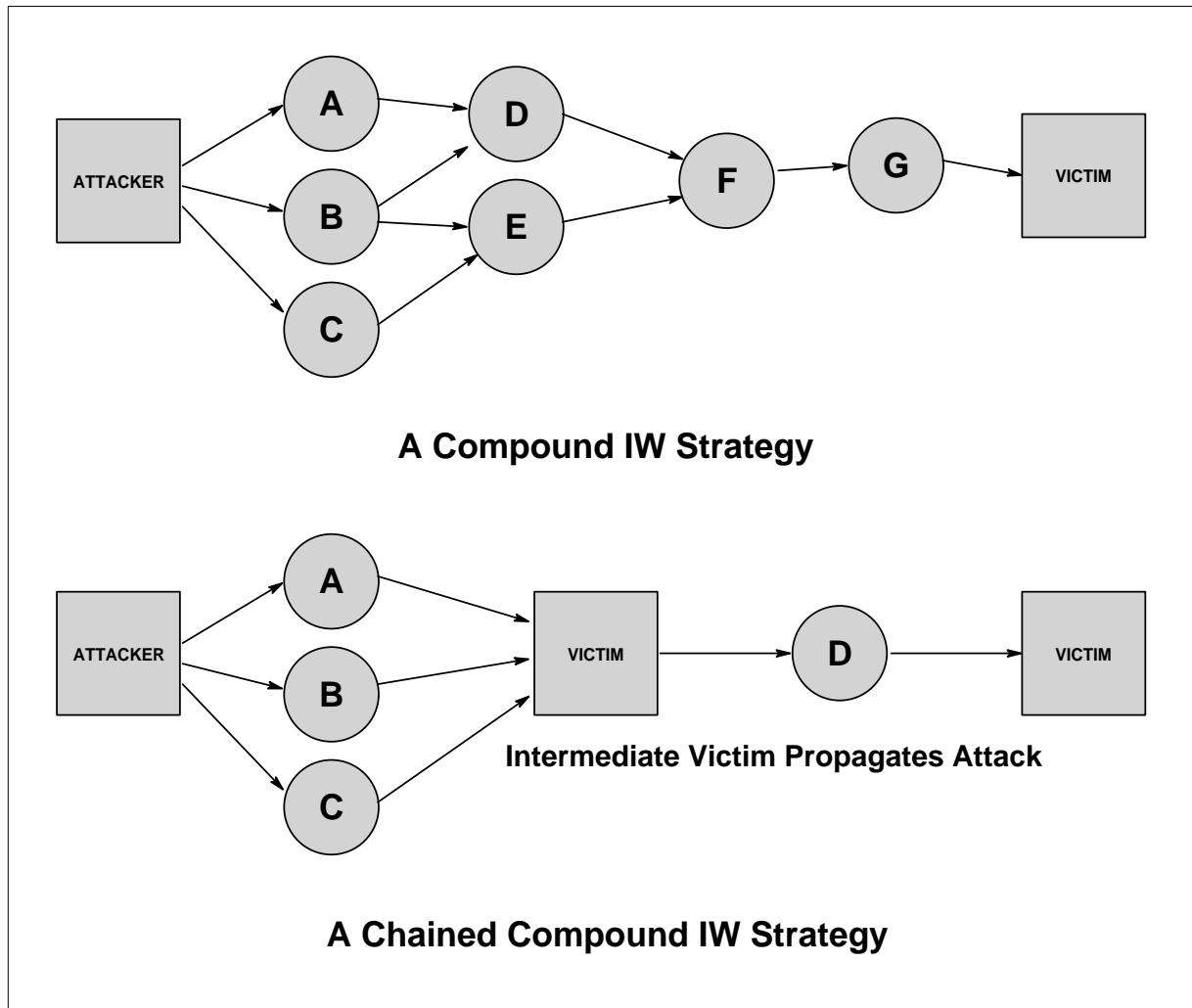


Figure 2: *Complex compound information warfare and chained compound information warfare strategies (Author).*

Because the precedence relationship is unidirectional in time, any compound strategy effectively forms a directed graph, which obeys the properties of directed graphs (Chartrand, 1977; Wilson, 1985).

Precedence relationships arise due to the state of the victim in the attack. In a compound strategy, antecedent strategies may not be feasible until a specific state of misperception or false belief has been established in the victim. A strategy may only be successful if this state change has taken place.

It is important to observe that an attacker may or may not perceive the state change in the victim's perception arising from an attack, compound or simple, and thus execute an antecedent strategy, compound or simple, after executing the precedent attack. This may or may not impair the success of the antecedent attack.

Concurrency:

Strategies between which no precedence relationship exists can be executed concurrently. There is no bound on the number of possible concurrent strategies.

Primary vs Supporting Strategies:

A strategy is said to be a supporting strategy if it supports the aim of another strategy, termed the primary

strategy. Supporting and primary strategies may or may not be concurrent. A non-concurrent supporting strategy is a strategy which must produce its effect before the primary strategy can be executed successfully.

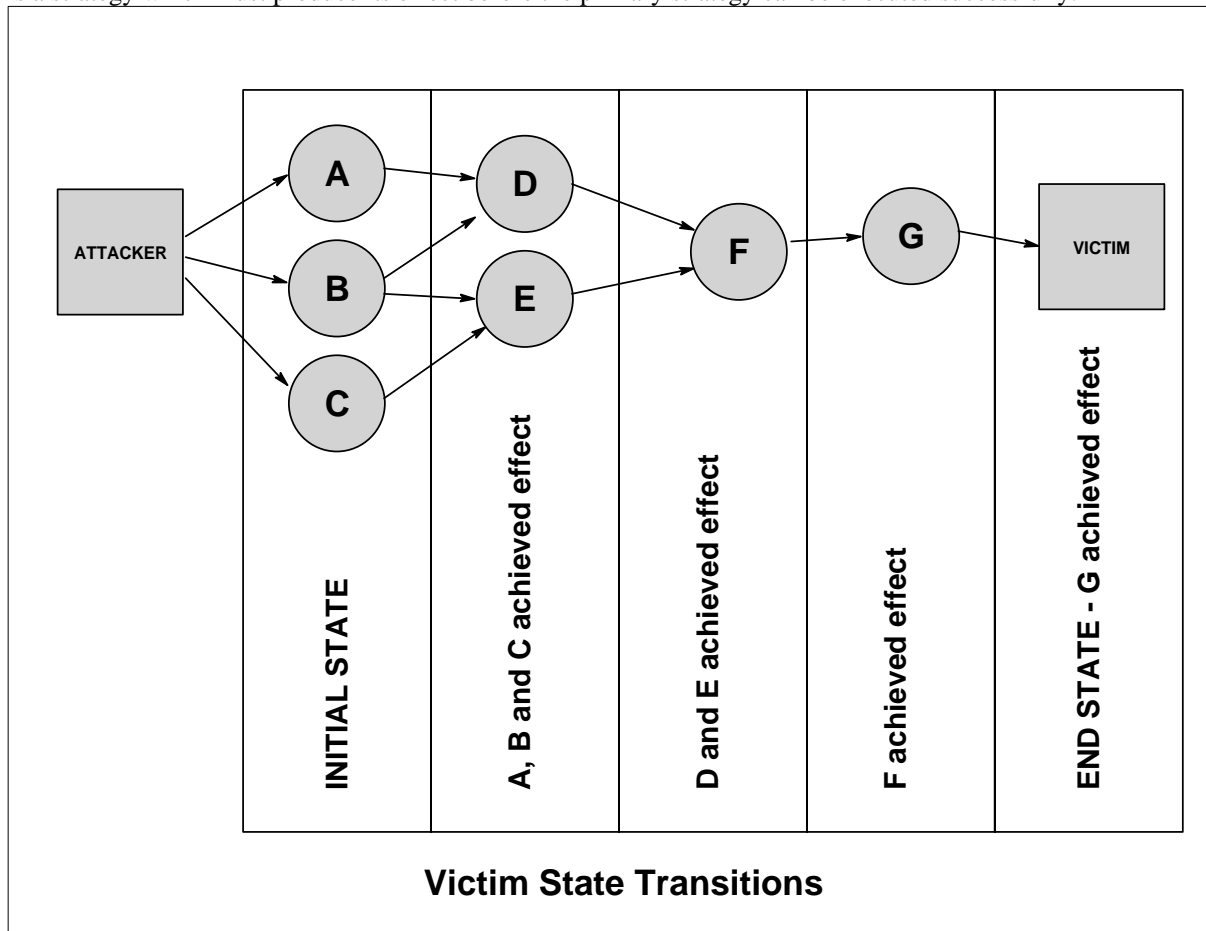


Figure 3: State transitions in a complex compound information warfare strategy (Author).

Chained or Sequential Strategies:

We define a chained or sequential strategy to be a compound strategy in which one or more intermediate victims are exploited. In such a strategy the first victim is employed as a conduit or proxy to propagate an information warfare strategy, or its effect.

An example of a chained or sequential strategy is the exploitation of media organizations by terrorist movements. The media organization is deceived into propagating a message targeted at a victim population, believing the message constitutes legitimate news.

Victim State:

The state of the victim is defined as the victim's belief at that point in time. A successful application of information warfare will effect an intended state change. An unsuccessful application may not produce a state change, or may by alerting the victim produce a state change in whatever other game the victim may be playing.

MODELLING COMPOUND STRATEGIES

A model for a complex compound strategy is a directed graph, in which precedence relationships exist between component canonical strategies. The topology of this graph is dependent upon the structure of the compound strategy.

Figure 2 illustrates two examples. The first (upper) example shows a compound strategy in which A, B and C are concurrent canonical strategies such as degradation and corruption. A and B are precedent strategies to canonical strategy D. B and C are precedent strategies to canonical strategy E. D and E are then precedents to F,

and F is a precedent to G, which effects the intended end state in the victim.

In this example G might be the canonical strategy of denial via subversion, and all of the precedents are strategies required to penetrate defences and enable G to be effected.

The second (lower) example shows a sequential or chained strategy in which A, B and C are concurrent strategies used to exploit the intermediate victim, who then propagates D to attack the victim and effect the end state.

The overall success of any complex compound strategy is measured by the end state of the victim. If the intended end state is not achieved, the strategy has failed.

In terms of systematically constructing a compound information warfare strategy, the starting point is the end state of the victim, and the intermediate states the victim must transition between from its initial state. These could be represented with any established technique for representing state transition diagrams. The condition which effects a state transition in the victim is the successful execution of the compound information warfare strategy which exists between two subsequent states. This is illustrated in Figure 3.

The *a posteriori* or forensic analysis of past attacks relies on establishing the precedence relationships and achieved states in the victim. The order in which specific compound or simple strategies were executed by the attacker is perhaps the most valuable tool the analyst has, as this allows attacks to be grouped, upon which the concurrent canonical strategies can be separated. The remaining step is to establish the specific aims of each of the constituent canonical and compound strategies.

As compound information warfare strategies have the properties of directed graphs, the behaviour of the cut vertex is of particular interest. A cut vertex is such a vertex, the removal of which partitions the graph into two smaller graphs (Chartrand, 1977; Wilson, 1985).

Any strategy, canonical or compound, which possesses the cut vertex property is a vulnerability within the overall compound information warfare strategy. The failure of this particular strategy, or its defeat by the victim, results in the total failure of the whole strategy.

The use of a systematic technique for the analysis of compound information warfare strategies offers advantages to attackers, defenders and third party observers. The third party observer might be a party who intends to either support or oppose the attacker or the victim.

The attacker can assess the robustness of the strategy at each state transition, by identifying whether the required strategies to effect that state transition have the cut vertex property, and thus represent a single point of failure for the strategy. Robustness could be improved by executing two or more concurrent compound strategies, all of which effect the same end state in the victim. This amounts to an application of the established reliability engineering technique of 'parallel redundancy' (Bazovsky, 1961). An excellent case study exists in the 1944 Fortitude operation (Ministry of Defence, 2004; Ricklefs, 1996).

A defender can assess the robustness of an attacker's strategy to identify where to best invest effort to disrupt the attacker's strategy. Knowing which specific strategies have the cut vertex property thus allows effort to be optimally focused in defeating the strategy.

The issue of defeating attacks in progress revolves around the victim's capability to identify the strategies being used to effect an attack. This can be problematic if the attack is well constructed and targets the victim's vulnerabilities, which the victim may or may not understand.

A victim or third party observer can derive useful information from the attacker's changes in strategy, as the attacker switches strategies upon achieving a state transition in the victim, or believing that such a state transition has occurred. The change in strategy will usually result in a different focus, and this can betray what the intended end state of the precedent strategy might have been.

STATE BASED MODELLING

Alternate mappings for this modeling technique exist. A state based mapping is such an alternative and may be attractive to users who are accustomed to using state transition diagrams, or project scheduling techniques such as PERT (Project Evaluation and Review Technique).

In a state based representation, the graph comprises nodes which represent initial, intermediate and end states for the victim, and directed edges which represent the strategies required to effect a transition from a preceding state. Rather than searching for cut vertices in the directed graph, analysis requires that bridges be identified (Chartrand, 1977; Wilson, 1985).

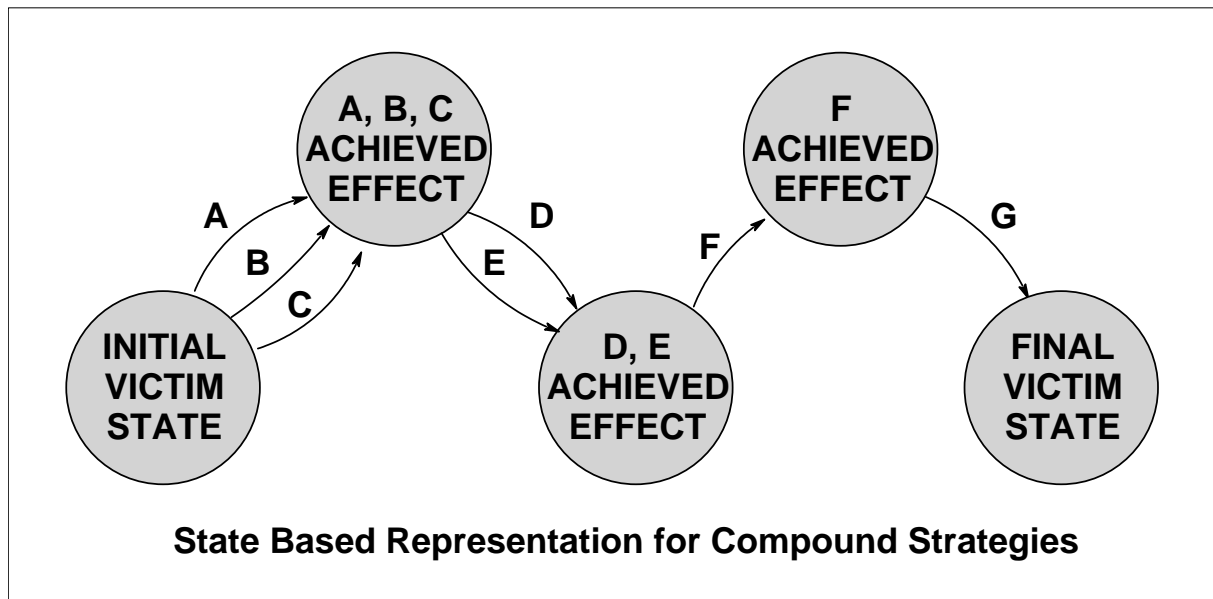


Figure 4: State based representation of the strategy depicted in Figure 2 and 3 (Author).

The limitation of the state based representation is that it will not always present the strategies used in an intuitive fashion. However, in compound attacks where multiple concurrent strategies may result in a multiplicity of intermediate states, this representation can be useful.

For instance, if we consider the compound strategy depicted in Figure 4, it is assumed that the state 'A, B, C achieved effect' requires that all three strategies be effective to achieve the desired state change. A similar strategy may consider a subset of the three precedent strategies to be adequate in achieving a desired victim state. Therefore this could be represented by four states rather than one state, these being 'A and B achieved effect', 'A and C achieved effect', 'B and C achieved effect' and 'A, B and C achieved effect'.

The choice of whether of a state based or strategy based graph is used to model a compound strategy will depend more than anything on user needs, and the architecture of the strategy being analysed. We can expect that specific areas of interest, such as modelling intelligence deceptions, mass media deceptions, or network attacks will prove to be more tractable using those representations which most intuitively capture the characteristics of the most common types of attack. Indeed, should software tools be developed or adapted for modelling such systems, then a well designed application would be capable of presenting the user with both representations.

An area not explored in this research to date is that of partial effects achieved by compound information warfare strategies. If the victim is an individual, such as is often the case in intelligence deceptions, then a partial effect could be a measure of the victim's confidence or belief in the veracity of a deception. If the victim is a group, as is typically the case in mass media deceptions, then a partial effect might be a measure of what fraction of the victim population has fallen for the deception, against what fraction has seen through or rejected the deception.

A related and no less important issue is the attacker's perception of the achieved effect resulting from the application of a compound information warfare strategy. In the context of a game or hypergame, (Kopp, 2003), the attacker's belief in the success, partial success, or failure of an information warfare strategy applied to a victim will determine whether the attacker assumes a state change has occurred in the victim, and thus whether an antecedent strategy should be pursued. In information warfare engagements which are symmetric, in the sense that both players are both attackers and victims, a state based model must encapsulate state changes in both players.

Empirical observation of many case studies of information warfare engagements, especially in the domain of

mass media deceptions, suggests that many players assume their victim is not playing an opposing game and thus that state changes in the victim do not occur. As a result, the deceptive strategy may be completely ineffective as the victim detects continuous changes in strategy.

VALIDATION OF MODELS

The validation of a model developed to represent a compound information warfare strategy *in progress* will vary in difficulty. This is due to varying complexities of strategies being played, and also due to varying quality and quantity of data supporting an effort to validate. This is a distinctly different problem to that of validating *a posteriori*, in a forensic analysis, a past strategy (Ministry of Defence, 2004; Ricklefs, 1996).

The latter case permits a simple process of analysing documents or events which detail specific antecedents, precedents, concurrent threads, and the intent behind the structure of the compound strategy.

Validating models for strategies *in progress* requires a different method. In situations where intelligence data, be it of human or machine origin, is available to penetrate defensive measures effected by the player under scrutiny, then such intelligence can be used to directly validate the intent and structure of the strategy.

In practice such intelligence may be partial or absent. At that point an analyst may have to approach the analysis problem with the perspective that the evolving strategy under analysis is uncertain. Effectively, the analysis will require the definition of several alternative models for the compound strategy, all sharing those features which existing data can logically support. As the strategy evolves further, alternatives will collapse as actions by the player contradict the respective alternative models.

It is important to observe that many deceptions involve mimicry and intentional emission of information by the deceiver. Therefore the structure of the strategy is exposed, even if its aim or end state may be unclear until the strategy develops into its latter states.

Conversely, compound deception strategies in which information is hidden completely will always present difficulties in analysis of the strategy, *a priori* or *in progress*. This is the essence of strategic surprise, as defined in the hypergame framework. Without evidence to prove that a deception strategy is underway, it is not feasible to perform analysis.

What is clear is that there is considerable opportunity for further research in the area of analytical modelling of compound information warfare strategies. The application of Bayesian techniques could prove to be especially valuable.

CONCLUSIONS

This paper has described a systematic analytical technique for modelling and analysing compound information warfare strategies.

This technique models compound strategies as directed graphs, with precedence relationships where applicable, and defines discrete state transitions in the victim as a measure of success. The concept of robustness in a compound strategy is introduced, this being defined as a measure of how few strategies in the compound strategy possess the cut vertex property.

The use of this systematic analytical method offers advantages to attackers, victims and observers. Future research is required to further explore techniques for the analysis of attacks in progress, and techniques for modelling partial effects upon victims, and the effects of belief in attackers.

REFERENCES

- Bazovsky I. (1961) Reliability Theory and Practice. Prentice-Hall, Inc, Englewood Cliffs, New Jersey, USA, 1961.
- Borden A. (1999) What is Information Warfare? *Aerospace Power Chronicles*, United States Air Force, Air University, Maxwell AFB, Contributor's Corner, URL: <http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html> [Date accessed: 01/09/04].
- Chartrand G. (1977), Introductory Graph Theory, Dover Publications, Mineola, New York, USA.
- Fraser N. M., Hipel K. W. (1984), Conflict Analysis, Models and Resolution. North-Holland, Elsevier Science Publishing Co., New York, USA.
- Haswell J. (1985) The Tangled Web: The Art of Tactical and Strategic Deception. Wendover, John Goodchild, 1985.
- Kopp C (2000), *A fundamental paradigm of infowar*, Systems, Auscom Publishing Pty Ltd, Sydney, NSW, February, 2000, pp 47-55, URL: <http://www.pha.com.au/papers/Kopp/IW-Paradigm-0200.htm> [Date accessed: 01/08/2005].
- Kopp C. and Mills B.I. (2002) Information Warfare and Evolution, *Proceedings of the 3rd Australian Information Warfare & Security Conference*, ECU, Perth. November, 2002. pp: 352-360.
- Kopp C. (2003) Shannon, Hypergames and Information Warfare, *Journal of Information Warfare*, **2**, 2: 108-118.
- Ministry of Defence (2004), *The Deception Plan - Operation Fortitude*, Commemorating the 60th Anniversary of D-Day, URL: <http://www.mod.uk/aboutus/dday60/fortitude.htm> [Date Accessed 20/10/2005].
- Ricklefs R.G. (1996), Fortitude South - D-Day Deception, *Military Intelligence Professional Bulletin*, Apr-Jun 1996, URL: <http://www.fas.org/irp/agency/army/mipb/1996-2/meeks.htm> [Date Accessed 20/10/2005].
- Widnall S. E., Fogelman R. R. (1997), *Cornerstones of Information Warfare*. Doctrine/Policy Document, United States Air Force.
- Wilson R. J. (1985), Introduction to Graph Theory, Third Edition, Longman House, Harlow, UK.

COPYRIGHT

[Carlo Kopp] ©2005. The author assigns the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to the Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the author.