

Shannon, Hypergames and Information Warfare

Dr Carlo Kopp

SCSSE, Monash University
carlo@mail.csse.monash.edu.au

Abstract

Shannon's Information Theory provides a robust and quantifiable model for explaining the fundamental paradigm of Information Warfare. This paper reviews the four canonical strategies of Information Warfare, in the context of Shannon's models and further extends these models into the domain of hypergame theory.

1. INTRODUCTION

For many years Information Warfare has existed without a robustly formulated fundamental mathematical theory to support it. Recently, Borden and Kopp related the four canonical Information Warfare strategies to Shannon's information theory, to provide a mathematically quantifiable theoretical basis for the discipline, refer (Kopp, 2000) and (Borden, 1999).

The limitation of this existing theoretical model is that it can model the effects of Information Warfare actions upon an information carrying channel, but provides little direct insight into how those actions might affect the outcome of an engagement between adversaries.

This paper will review the existing model, based upon Shannon's theory, and further extend it through the application of *hypergames*. In doing so it will provide a much more powerful technique for explaining and modelling the system level effects of Information Warfare actions.

2. SHANNON AND INFORMATION WARFARE

Perhaps the most widely accepted formal definition of Information Warfare is the model asserted by the United States Department of Defence¹ :

'Information Warfare is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions'.

This definition describes Information Warfare in terms of 'actions' executed to achieve a sought outcome - denial, exploitation, corruption and destruction of an opponent's 'information' and related functions, and prevention of such 'actions' executed by an opponent.

Information in this instance is not defined in directly quantifiable terms. Borden and Kopp have both asserted that the basis of a quantifiable model for 'information' in this context should be based upon information in Shannon's model for a communication channel, (Borden, 1999), (Kopp, 2000), defined in (Shannon, 1948), refer Fig 1.

Shannon's model describes the system in terms of an 'information source' which produces messages, a 'transmitter' which operates upon these messages to convert them into a form suitable for communication over a 'channel', i.e. the medium of the transmission, upon which the messages are reconstructed by a 'receiver' which then provides these messages to the 'destination' entity. The 'noise source' in Shannon's model introduces errors into the channel.

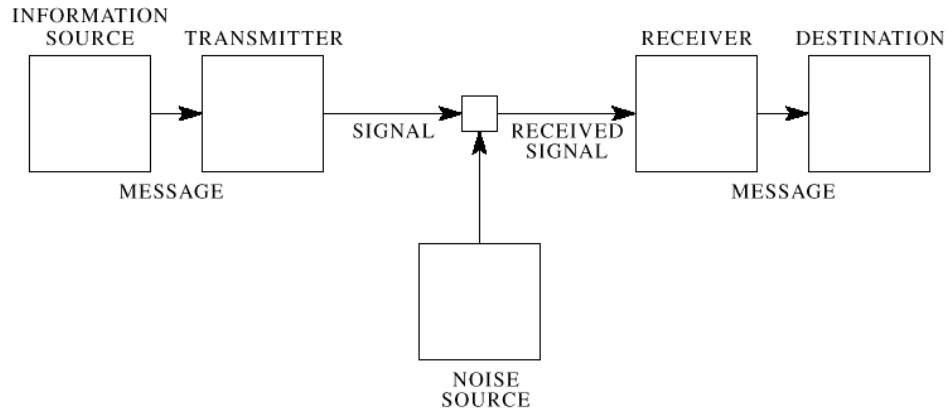


Figure 1: *Shannon's model for communication channel (Shannon, 1948).*

Shannon showed that the 'capacity' of a channel to transmit information across a channel of a given bandwidth in the presence of noise was bounded by the relationship:

$$C = B \cdot \log_2 (S/N)$$

Where C is channel capacity, B is channel bandwidth, S is signal power and N is noise power. Shannon's relationship is the basis of modern communications theory.

Shannon's original definition of channel behaviour in the presence of noise was framed in the context of a communications systems. In this context, Signal to Noise ratio (S/N or SNR) and bandwidth are measures of channel 'quality', and achievable transmission data rate and error rate are constrained by such. Decreasing signal power, decreasing bandwidth and increasing noise power all serve to diminish the useful capacity of the channel.

In the context of Information Warfare, the 'message' and 'transmitter' components of the model, and the receiver and destination components have broader meanings. Consider for instance the radar detection model, where a radar illuminates a target to establish its position, kinematic parameters and possibly even identity. In this model the 'message' is encoded in the modulation and timing of the power backscattered from the target, while the 'transmitter' is the reflecting body of the target vehicle, which is supplied with power by the microwave source in the radar producing the illumination. In this example the attacker may degrade the S/N of the radar by applying a microwave absorbent coating to his vehicle, and in doing so hide the vehicle's radar return in the background noise and noise floor of the radar's receiver.

Information Warfare in the most fundamental sense amounts to manipulation of a channel carrying information in order to achieve a specific aim in relation to an opponent engaged in a survival conflict, refer (Borden, 1999), (Kopp, 2000).

Borden describes this effect as the 'battle for bandwidth' - a contest over the available capacity in a channel carrying informationⁱⁱ.

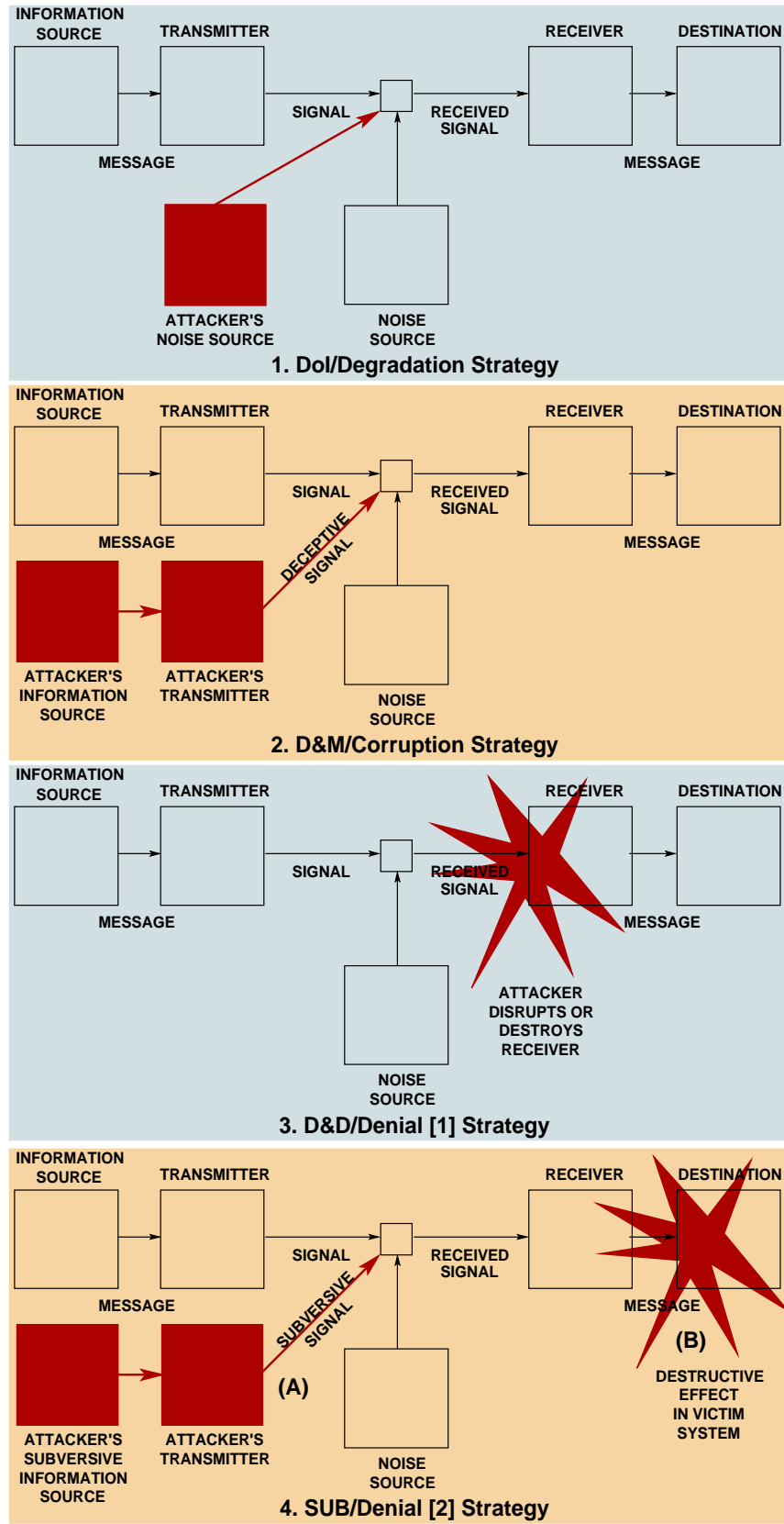


Figure 2: The four canonical offensive Information Warfare strategies (Author).

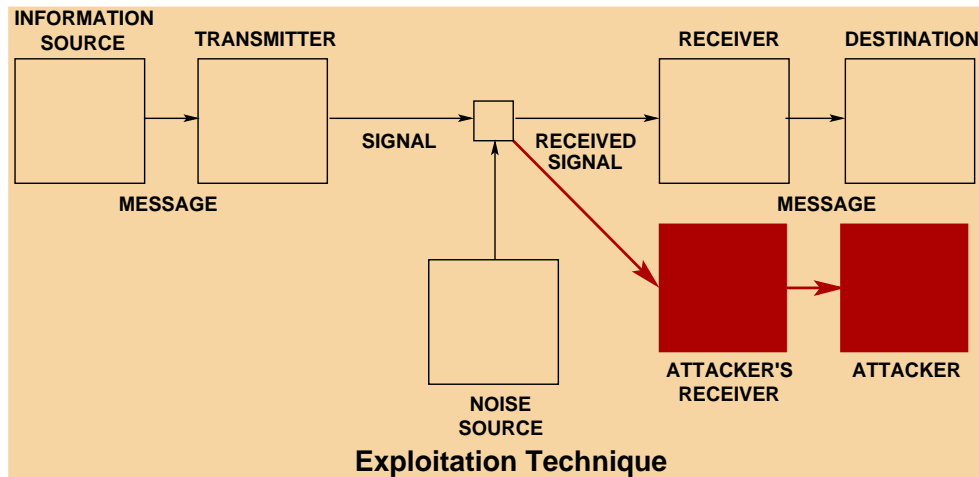


Figure 3: *Exploitation as an Information Warfare technique (Author).*

For practical purposes, the available channel capacity for any given information gathering, processing and transmission function is actively manipulated by players who will apply a range of measures to gain an advantage over their opponent. The advantage lies in improving one's own available capacity, while preventing like action by an opponent.

Four canonical offensive Information Warfare strategies have been identified (Kopp, 2000) and (Borden, 1999), yielding two models which overlap but essentially encapsulate the same effects:

1. **Denial of Information / Degradation or Destruction (US DoD)**, i.e. concealment and camouflage, or stealth; DoI amounts to making the signal sufficiently noise-like, that a receiver cannot discern its presence from that of the noise in the channel.
2. **Deception and Mimicry / Corruption (US DoD)**, i.e. the insertion of intentionally misleading information; D&M amounts to mimicking a known signal so well, that a receiver cannot distinguish the phony signal from the real signal.
3. **Disruption and Destruction / Denial [1] (US DoD)**, i.e. the insertion of information which produces a dysfunction inside the opponent's system; alternately the outright destruction of the receiver subsystem; D&D amounts to injecting so much noise into the channel, that the receiver cannot demodulate the signal.
4. **SUBversion / Denial [2] (US DoD)**, i.e. insertion of information which triggers a self destructive process in the opponent's target system; SUB 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 machineⁱⁱⁱ.

The US DoD taxonomy includes Exploitation as a fourth 'Attack Measure', Exploitation defined as gathering an adversary's flow of information to facilitate friendly information generation. Exploitation amounts to attaching a receiver in parallel with the opponent's receiver. Since it does not in itself produce an immediate causal effect in the function of the target channel, it cannot be classified as an offensive Information Warfare strategy in the sense of the four defined strategies. Rather, it is an information gathering 'technique', albeit one which may facilitate the application of an offensive Information Warfare strategy. The models for these strategies, and Exploitation, are depicted in Figures 2 and 3.

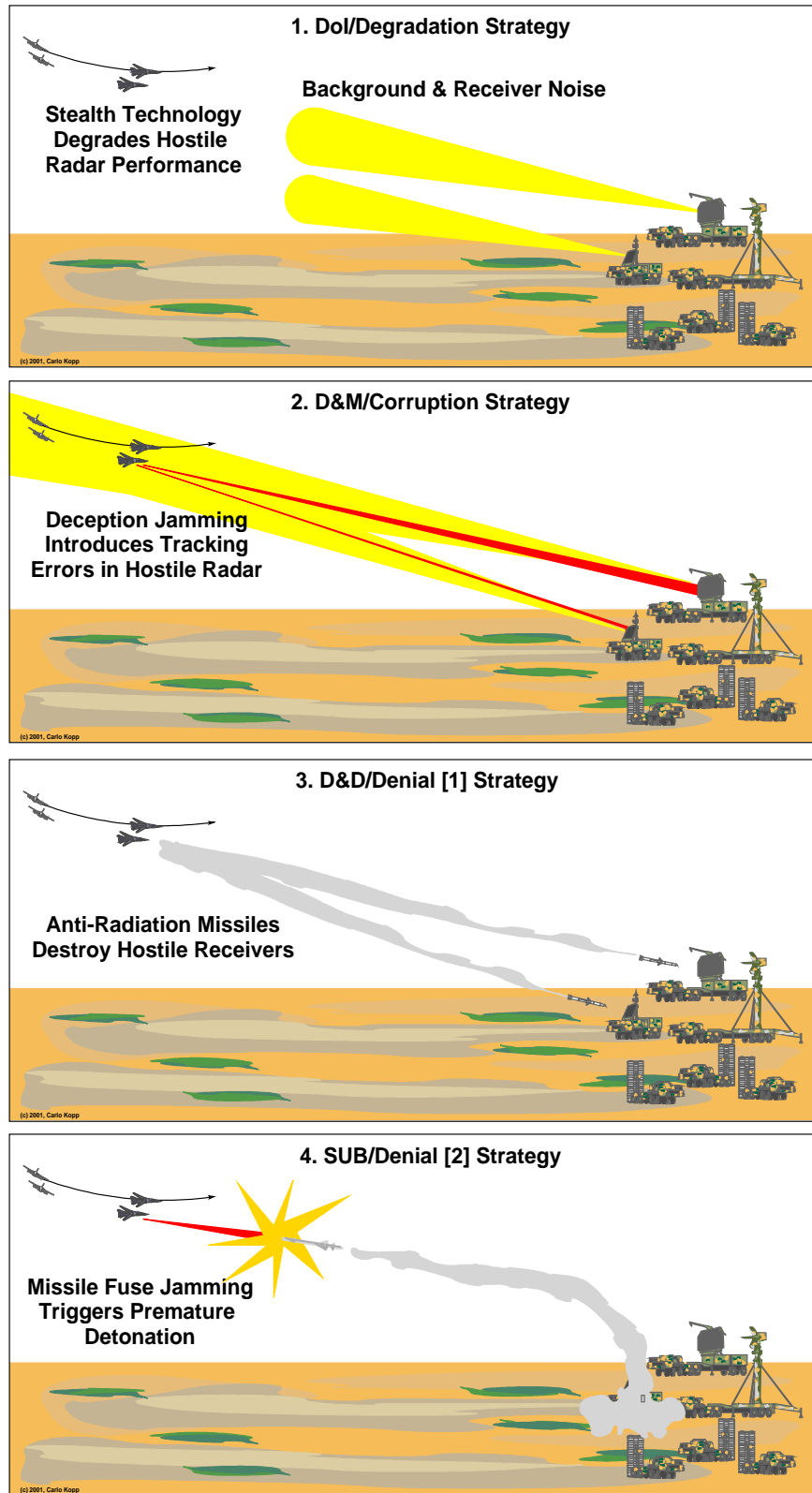


Figure 4: Contemporary examples of the four canonical offensive Information Warfare strategies in the Electronic Attack domain (Author).

As with the preceding example of the radar system, in the interests of generality the depicted models separate the attacker's message generation and transmitter functions from the channel proper. This reflects the reality that the topology of the physical system may not map directly on to the channel model. Strategy [1.] could for instance involve a support jamming aircraft flying at a distance of several miles from the target aircraft it is protecting by jamming the victim radar. The principal distinction between the Kopp model and the US DoD model is one of definition - the US DoD model lumps destruction of the opponent's receiver function and destruction of the opponent's system through subversion into one category, while the US DoD model includes passive exploitation as an active offensive measure. While the US DoD model is coarser in its distinctions between the respective strategies, it remains largely adequate for most applications.

A range of contemporary examples describing the four strategies are discussed in (Borden, 1999) and (Kopp, 2000). There is no shortage of case studies in the domain of electronic warfare and electronic attack, of interest is the fact that all basic electronic warfare and electronic attack techniques predate Shannon's research by several years. Contemporary examples are depicted in Fig 4, with more detailed discussions in references (Fitts, 1980), (Schlesinger, 1979), (Knott, 1985), (Knott, 1985) and (Ball, 1985).

Shannon's information theory provides a powerful model for describing the interaction between adversaries applying Information Warfare techniques and the information carrying channel itself. What the model cannot describe is how the manipulation of the channel may be reflected in the behaviour of the respective adversaries.

3. HYPERGAMES AND INFORMATION WARFARE

An alternate approach to modelling the fundamental paradigm of Information Warfare can be found in game theory, specifically in *hypergames*^{iv}.

Hypergames are games in which the respective adversaries (players) may not be fully aware of the nature of the engagement they are participating in, or indeed that they are actually participating in an engagement. Characteristics of hypergames include:

1. Players may have false perceptions of the intent or aims of the other players.
2. Players may not understand the choices available to other players.
3. Players may not know who other players in the game may be.
4. A player may be subject to one or more of the previous misperceptions of the game.

In practical terms, players in hypergames have perceptions of the engagement which may not reflect the true nature of the engagement, resulting in decisions and outcomes which may not reflect the interests or indeed intent of the players. Refer Fig 5.

In classical game theory players typically have *perfect information* about the state of the game, there are no misperceptions of previous moves. In the hypergame model, the players' perceptions of reality are generally not considered to map one to one on the reality of the game they are parties to.

A general description of a hypergame is given in (Fraser, 1984), in which n players each perceive a particular game:

$$H = \{G_1, G_2, G_3, \dots, G_n\}$$

Each game perceived by the participating players can be described with a set of outcomes, as perceived by that player:

$$G_i = \{O_1, O_2, O_3, \dots, O_m\}$$

Each outcome, in turn, comprises a set of possible actions (moves) by respective players, as perceived by player i :

$$O_i = \{\{A_1, A_2, \dots, A_q\}_1, \{A_1, A_2, \dots, A_p\}_2, \dots, \{A_1, A_2, \dots, A_r\}_n\}$$

Each player will seek to execute actions which yield a set of outcomes most favourable to that player, should we assume the player is rational.

This model can be related to the well established Boyd *Observation-Orientation-Decision-Action Loop* model insofar as a player's perception of the game is the outcome of the *Observation-Orientation* phases of the loop, and the *Decision-Action* phases of the loop reflect the choices made by the player, based upon the player's perception of the game and what constitutes the best choice to make. Refer (Boyd, 1986).

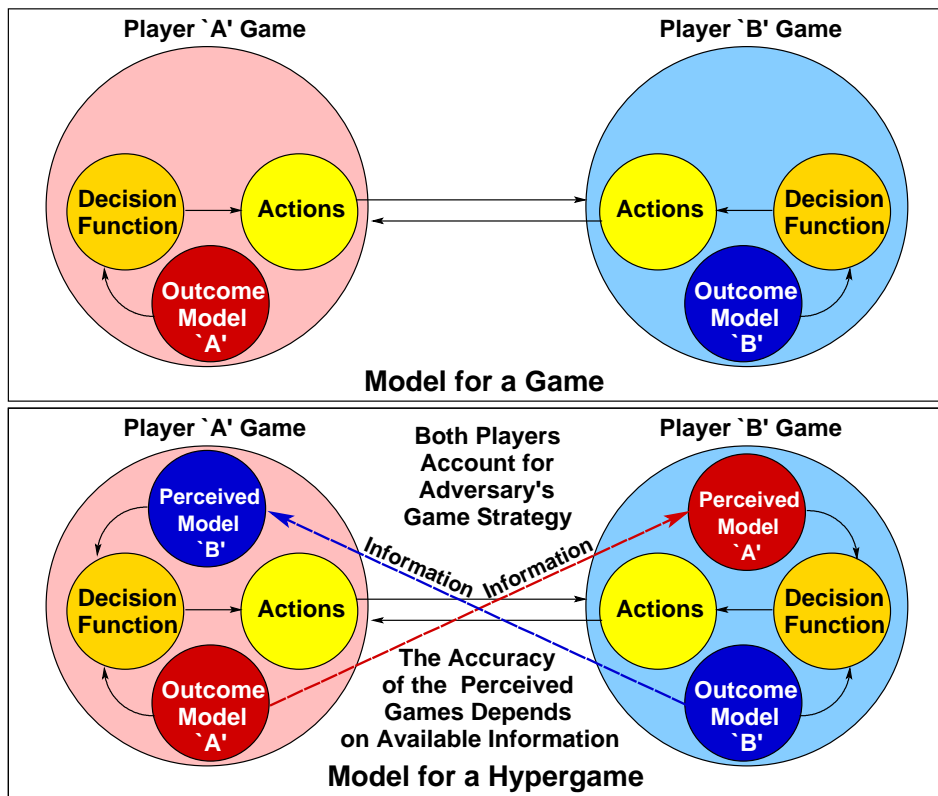


Figure 5: In a hypergame the players perceive their opponents' games. How accurate that perception might be depends on the information available to respective players. Inaccurate information leads to a misperception of the game state and may lead to actions which do not gain the player an advantage (Author).

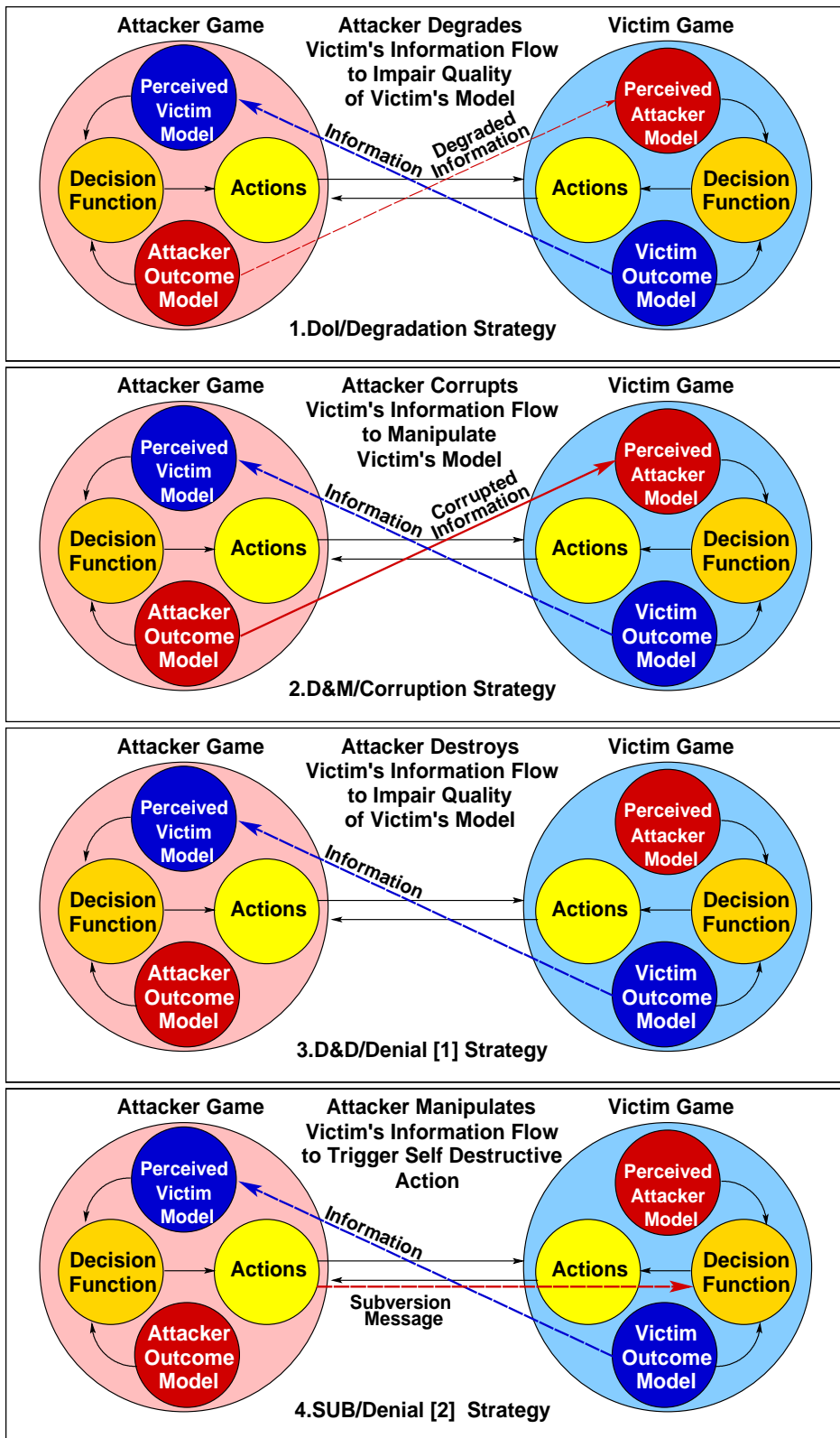


Figure 6: Hypergame models for the four canonical Information Warfare strategies (Author).

In the context of a hypergame, Information Warfare is a means to an end - that end is the alteration of an opposing player's perception of the game in a manner which yields an advantage to the player who applies the means of Information Warfare.

A special case in the hypergame model is *strategic surprise*, where a player may be wholly unaware of another player's presence in the game, or may be unaware of action other players have the option of taking.

It is worth exploring the four canonical strategies in the context of a simple two player hypergame:

1. **Denial of Information / Degradation or Destruction (US DoD)**, this IW strategy is central to hypergames in which either the presence of a player, or the intent of a player is to be concealed from another. Strategic surprise is frequently contingent upon the successful execution of this strategy.
2. **Deception and Mimicry / Corruption (US DoD)**, is applied in a hypergame in order to alter another player's perception of the game at hand. It amounts to directly changing another player's perception of the game.
3. **Disruption and Destruction / Denial [1] (US DoD)**, is applied by a player in a hypergame to prevent another player from perceiving the state of the game. Unlike DoI, D&D can show the intent and possibly identity of the player using it, and thus may convey this information to the victim player.
4. **SUBversion / Denial [2] (US DoD)**, is a strategy where a unilateral action by a player alters the perception of the situation by a victim player in a manner which elicits a self destructive unilateral action by the victim player.

Clearly, the hypergame model is a very good fit to the fundamental paradigm of Information Warfare, insofar as the four canonical strategies map directly into models which are well represented by hypergames, refer Fig 6. Higher level hypergames, in which a player's perception of an opponent's perceptions are incorporated into the model, provide an important refinement.

While the use of Shannon's capacity model provides an important tool for modelling the immediate effect of an Information Warfare action in terms of the flow of information into a victim system, it cannot model the effects which may flow from this action. Conversely, while a hypergame is not a good model for describing the immediate effect of an Information Warfare action, it is a good model for describing the possible results of such an action.

This is of key importance to practitioners of Information Warfare, insofar as which of the four canonical strategies, or combinations thereof, are most suitable for any given scenario can only be determined by the careful use of both models. In an environment where effects based targeting is important, the use of a hypergame model can provide a warfighter with a high level of confidence that the intended effect may indeed be achieved.

4. CONCLUSIONS

This paper has explored the modelling of the four canonical strategies in Information Warfare using Shannon's channel capacity model, and using the model of a hypergame.

Both of these models are powerful tools for understanding the basic nature of Information Warfare, yet also provide a means for directly quantifying the effects of an Information Warfare action, and determining likely outcomes of an Information Warfare action, respectively.

The combined use of these techniques offers a robust means of modelling the effects of an Information Warfare action along the whole chain comprising the information carrying channel and the decision processes of an opponent, thus permitting the modelling of substantial proportions of an opponent's *Observation-Orientation-Decision-Action* loop.

This technique can be further extended into the domain of higher level hypergames, in which the mutual perceptions of opponents' perceptions are modelled. This is an area for future research.

REFERENCES AND BIBLIOGRAPHY

- Ball R. E. (1985), *The Fundamentals of Aircraft Combat Survivability Analysis and Design*. American Institute of Aeronautics and Astronautics, Inc., New York.
- Borden A. (1999), What is Information Warfare? *Aerospace Power Chronicles, United States Air Force, Air University, Maxwell AFB*, Contributor's Corner:
<http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html>, 2 November.
- Boyd J.R., Col USAF, (1986), *Patterns of Conflict*, Briefing Slides, December, 1986, Washington DC, USA.
- Fitts R. E. (Ed). (1980), *The Strategy of Electromagnetic Conflict*. Peninsula Publishing, Los Altos, Ca.
- Fraser N. M., Hipel K. W. (1984), *Conflict Analysis, Models and Resolution*. North-Holland, Elsevier Science Publishing Co., New York, USA.
- Knott E. F., Schaeffer J. F. and Tuley M. T. (1985), *Radar Cross Section, First Edition*. Artech House, Dedham, Ma.
- Knott E. F., Schaeffer J. F. and Tuley M. T. (1993), *Radar Cross Section, Second Edition*. Artech House, Dedham, Ma.
- Kopp C. (2000), Information Warfare: A Fundamental Paradigm of Infowar. *Systems: Enterprise Computing Monthly, Auscom Publishing, Pty Ltd, Sydney, Australia*, February:46–55, 2000. Posted at <http://www.infowar.com/>, April.
- Schlesinger R. J. (1979), *Principles of Electronic Warfare*. Peninsula Publishing, Los Altos, Ca.
- Shannon C. E. (1948), A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27:379–423, 623–656, July, October.
- Widnall S. E., Fogelman R. R. (1997), Cornerstones of Information Warfare. Doctrine/Policy Document, United States Air Force.
-
- ⁱ Cited in (Borden, 1999), refer (Widnall, 1997).
- ⁱⁱ Unpublished correspondence between the author and Dr A. Borden, 2001.
- ⁱⁱⁱ The Turing machine model is used for generality as any computer can be mapped into a Turing machine. A less rigorous but more intuitive definition is 'altering the program on the opponent's hardware or wetware so as to alter the behaviour of the victim system'.
- ^{iv} Bennett, cited in Fraser and Hipel's *Conflict Analysis* refer (Fraser, 1984).