

Classical Deception Techniques and Perception Management vs. the Four Strategies of Information Warfare

C. Kopp

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

Abstract

The use of deception techniques for intelligence operations, strategic and tactical deception in war, politics, business and media manipulation is well established and well documented. This paper analyses established deception techniques in the context of the four canonical strategies of Information Warfare, to establish an information theoretical and game theoretical framework for future modelling and analysis.

Keywords

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

INTRODUCTION

Established literature on the theory of deception largely predates the formal mathematical formulation of Information Warfare techniques. As a result a large body of work exists, which has not been mapped into a form suitable for mathematical or computer modelling (Borden, 1999; Kopp, 2000).

Deception is an important aspect of Information Warfare, and as such qualifies as a biological survival mechanism, evolved for the purpose of gaining an advantage in a survival game (Kopp, Mills, 2002).

In this context, deception is characteristically used to support a game, or more frequently a higher order hypergame, played out between participants in the survival contest (Kopp, 2003).

Players of games or hypergames specifically employ Information Warfare strategies, including deception, to alter an opponent's perception of the game to so gain an advantage. In effect, the player using deception aims to specifically manipulate the opponent's game strategy by presenting deceptive information which alters the opponent's hypergame model of the player's subgame.

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.

This paper will first survey 'classical' deception techniques, as employed in intelligence and other deceptions, media manipulation techniques, employed in politics and war, and then map these respectively into models based on the four canonical Information Warfare strategies.

CLASSICAL DECEPTION TECHNIQUE

One of the best summaries of classical deception techniques, as employed in the military environment, is that provided by Haswell (Haswell, 1985).

Haswell defines five 'deception techniques' and two 'tactical methods', which in implementation are supported by seven 'principles of deception'. The former amount to applications of the four canonical strategies, while the latter amounts to a methodology for defeating an opponent's efforts to unmask the deception.

Haswell's five deception techniques are defined thus:

1. **The Lure** – this technique presents the opponent with a sudden advantage they may exploit.
2. **The Repetitive Process** – this technique conditions the opponent by repetition to accept harmless behaviour that is used as a cover for subsequent operations.
3. **The Unintentional Mistake** – this technique leads an opponent to believe that valuable information has come into his hands by mistake, for instance by negligence or incompetence.
4. **The Obvious Solution** – this technique provides deceptive information to support the idea that the obvious method will be used, while hiding information related to the actual method.
5. **The Piece of Bad Luck** – this technique is similar to the Unintentional Mistake, except the bad luck cannot be attributed to anyone.

Haswell's tactical methods are then defined as:

1. **Doctrine of Indirect Approach** – this method aims to avoid a frontal assault against an entrenched opponent, by convincing them the attack will come from elsewhere.
2. **Exploitation of the Impossible** – this method is intended to take an opponent by surprise by doing what the opponent believes is impossible.

A key feature of all of these techniques and methods is that an opponent's correct beliefs about a situation are either altered to be incorrect, or incorrect beliefs are reinforced.

The seven principles of deception defined by Haswell aim to provide, in practical terms, an algorithm for implementing the five techniques and two methods:

1. **Preparation**
 - Deception needs a well defined aim and to be directed at a target.
 - Needs detailed knowledge of the target.
 - Plan the entire scheme and consider the target's reaction to it.
 - Also plan the groundwork for the deception.'
2. **Credibility**
 - Deception must never seem incongruous or illogical. It must be feasible.
 - It should be in line with what the target expects to happen.'
3. **Multi-Channel Support**
 - All the false information on all channels must support the deception.
 - Channels must also conform to each other.
 - Positive to draw target's attention, negative to repel attention.'
4. **Centralised Control**
 - Deception schemes should be centrally controlled to avoid confusion.
 - All schemes must be centrally controlled and the level of control (headquarters) determined by the number of units involved in the plan.'

5. **'Security'**

- Detailed knowledge of deception limited to the smallest number of people. ·
- Knowledge on a need to know basis.'

6. **'Flexibility'**

- Deception plan should be flexible to take advantage of unforeseen developments or to abandon it without revealing the aims of the deception plan.'

7. **'Coordination'**

- Individuals need to know what they must do and when.'

The classical model of deception technique, presented by Haswell, must be analysed in the context of a hypergame., rather than simple game. This is because players in such deception techniques invariably invest considerable effort into manipulating or even controlling the opposing player's perception of their own play, and attempting to unmask the opponent's efforts to manipulate or control their own perceptions of the opponent's play.

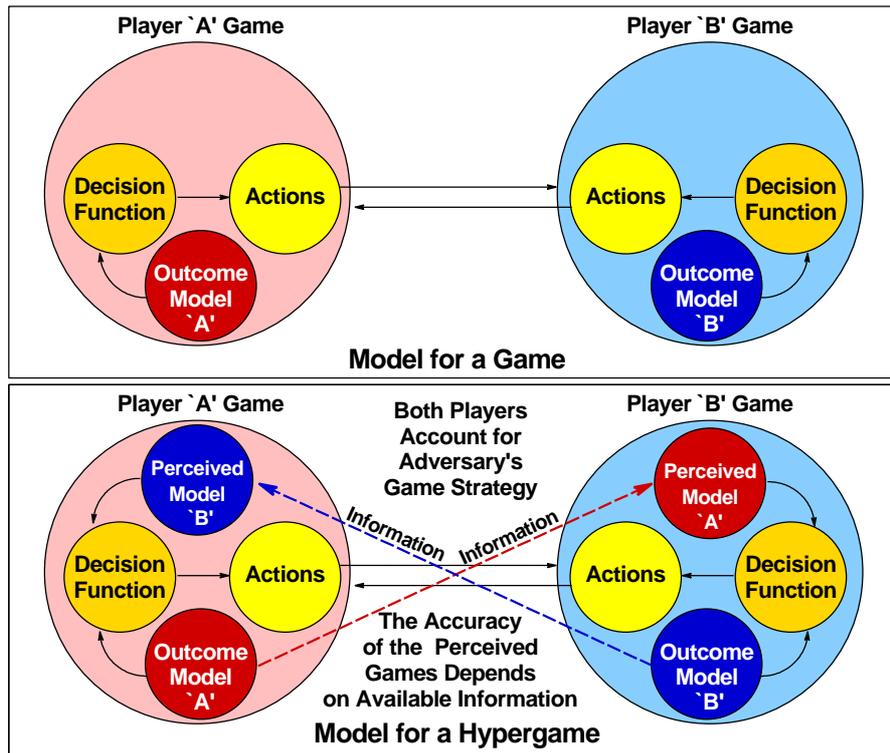


Figure 1: In a hypergame the players perceive their opponents' games. How accurate that perception might be depends on the information available to respective players. Inaccurate information leads to a misperception of the game state and may lead to actions which do not gain the player an advantage. Both models are structured around Boyd's Observation Orientation Decision Action loop (Author).

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 (Fraser, 1984):

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 the simplest of terms, the hypergame is the framework or context in which specific strategies or combinations of strategies are employed to effect the deception. Indeed, the two 'tactical methods' presented by Haswell are both instances of hypergames, the latter of the two being the 'strategic surprise' play (Fraser, 1984).

It is important to recognise that the four canonical strategies of information warfare are effectively mutually orthogonal primitives, which can be combined in an arbitrary manner to form a *compound strategy* (Kopp, 2005). Exploring many empirical case studies indicates that compound strategies are used very often in nature (Kopp, Mills, 2002).

Technique	Primary Strategy	Supporting Strategy	Notes
The Lure	Corruption/Mimicry	Degradation/Denial	Introduce new misperception
The Repetitive Process	Corruption/Mimicry	Degradation/Denial	Reinforce existing misperception
The Unintentional Mistake	Corruption/Mimicry	Degradation/Denial	May be used to support Denial via subversion
The Obvious Solution	Corruption/Mimicry	Degradation/Denial	Reinforce existing misperception
The Piece of Bad luck	Corruption/Mimicry	Degradation/Denial	May be used to support Denial via subversion

Table 1: *Canonical forms of the classical deception techniques.*

The first of the five classical deception techniques, the Lure, presents the victim with an attractive opportunity to improve their position, which the victim is compelled to exploit. The victim perceives an advantageous situation which has been fabricated to weaken their position. At the most basic level this play qualifies as an example of the corruption strategy, as mimicry is employed to create a perception of an advantageous situation which does not exist. Degradation may be employed as a supporting strategy, by employing camouflage techniques to hide information which may expose the ruse. Therefore we can identify two specific forms in the Lure. The canonical form is where corruption is used alone, the compound form where degradation is employed to defeat defensive information gathering by the victim player.

The second of the five classical deception strategies, the Repetitive Process, is similar to the Lure in having the same compound and canonical forms. Its implementation differs as it is intended to deceive by mimicking behaviours which are not characteristic of preparations for an attack. The aim of the Repetitive Process is different from the Lure, since the latter is designed to compel an opponent to make a move in the game, whereas the former is intended to conceal preparations for a move by the attacker.

The third of the five classical deception strategies, the Unintentional Mistake, is a mimicking technique and thus also qualifies as corruption. The player mimics a mistake and the victim is compelled to exploit the mistake. More than often this play will include concealment or camouflage as a supporting strategy, and thus exists in both canonical and compound forms.

Some case studies show the use of the Unintentional Mistake as a technique used to introduce a false belief that intelligence sources being used by the victim are in fact double agents, when this is not so (Haswell, 1985). As a result the victim will destroy its intelligence network in an effort to remove the believed to be compromised agents. If the Unintentional Mistake is used for this purpose, it is part of a larger compound strategy, in which corruption and degradation are used as supporting strategies for a denial game, in which the victim is subverted into using internal resources to self destruct.

The fourth of the five classical deception techniques, the Obvious Solution, is prima facie an example of corruption and degradation, in that mimicry or concealment will be employed to hide the real intent from a victim. It aims to reinforce an existing but incorrect perception by the victim that the obvious play is the correct play. Whereas earlier plays either aim to implant a false perception or aim to conceal, the Obvious Solution is

mostly intended to reinforce an existing but incorrect perception by the victim. Knowledge of the victim's actual perception is often valuable if this play is to be implemented. Many good historical case studies can be found in the Ultra program and related exploitation of Enigma intercepts.

The fifth of the five classical deception techniques, the Piece of Bad Luck, is a form of the Unintentional Mistake and thus a canonical or compound strategy using corruption and degradation. The implied cause of the 'unintended' disclosure is different.

The seven principles presented in the classical model are mostly designed as mechanisms to defeat defensive measures by potential victims. In any environment where deception is expected by an opponent, players will invest considerable effort in attempting to validate newly acquired information. Methods designed to ensure logical consistency and multi-channel support for a deceptive play will defeat attempts at detecting deception by comparing multiple information sources and their relative content. Some interesting case studies of the application of the five deception techniques and seven principles are detailed in (Hansen, 2002), (Kern, 2003), (Kerbel, 2004), (Grabo, 2000) and (Mendez, 2000).

MASS MEDIA PERCEPTION MANAGEMENT

The use of mass media 'perception management' techniques has a long and colourful history. Without doubt the most notable examples are Germany's Third Reich, the Soviet Union and related Warsaw Pact efforts, and more recently, Al Qaeda and affiliated Islamo-fascist entities. What is characteristic of all three of these groups of players is a specific pattern of technique and the use of a sustained and internally consistent long term deception campaign, characteristically targeted at followers of the regime or movement. More than often 'perception management' techniques intended to attack opponents of such regimes are unique, and indeed different from those targeting the captive population.

If we model the victim population as the target of a systematic and organised campaign of deception by the regime or movement, a number of key strategies and principles become apparent.

The first is that such a campaign will mostly have these attributes:

1. Preparation - the deception campaign has well defined aims in reinforcing the cohesion of the victim population, and reinforcing the ideological or political position propagated by the regime.
2. Credibility - the deception campaign is usually internally consistent, and if modelled as a graph, displays arguments which follow cycles designed to avoid contradictory ideas or facts. More than often existing victim population prejudices or expectations are incorporated in the deception to reinforce its credibility.
3. Multichannel support – multiple mutually supportive deceptive arguments and fabricated facts are used to reinforce the deception campaign, and defeat attempts by the victim population to unmask the deception. Soviet and Nazi rewriting of official histories to maintain logical consistency and avoid contradictory facts makes for an excellent case study.
4. Centralised control – entities such as propaganda ministries, propaganda bureaux or propaganda arms of political parties or movements are employed to provide centralised control of the deception campaign.
5. Security – the nature of the deception campaign, i.e. knowledge of the ground truth as compared to the deceptive messages, is usually only known to a small fraction of the leadership group.
6. Flexibility – the deception campaign typically adapts and evolves over time, as it adapts to changing circumstances. A good example is the era of Soviet purges during the 1930s, when new and 'unexpected' class enemies and traitors were 'exposed' over time.
7. Coordination – party organisations and propaganda ministries/bureaus characteristically follow rigid hierarchical patterns of organisation to provide consistent and synchronised distribution of deceptive messages to the victim populace.
8. Concealment – information which could contradict the deception campaign is hidden or destroyed.
9. Untruthful statements – untruthful statements are fabricated with the aim of mimicking the ground truth.

A myriad of examples which validate this model exist in Soviet and Nazi regime histories, as well as recent Jihadist and Al Qaeda propaganda targeting Muslim populations. Specific case studies of interest are discussed in (Holland, 2001), (Fischer, 1999), (Grabo, 2000) and (Goebbels, 1934; 1938; 1940; 1943; 1944; 1944).

Importantly, there is a one to one mapping between the fundamental models used in classical deception technique, and the highly structured fabrication and distribution of deceptive propaganda targeted at a victim population by the example regimes or movements. At the most fundamental level of canonical and compound Information Warfare strategies and supporting techniques, internal propaganda aimed at a victim population

is indistinguishable from classical deception techniques employed in intelligence or military operations. For all intents and purposes, the example regimes/movements conducted or are conducting sustained deception campaigns against the victim population, implicitly treating the victim population as an opponent in a game.

Deception and propaganda campaigns targeting the populations of developed democracies, in a globalised and highly networked world, follow a different pattern but also exploit classical deception technique. The principal distinction in application is a result of the lack of structural control over global media organisations and networks, which are not part of the regime or movement's internal organisation.

The result of this is that media organisations must be subjected to a deception effort designed to compel them to become a delivery mechanism for deceptive messages targeting the victim population.

Most modern electronic and print media organisations are primarily focussed on the delivery of 'infotainment' rather than dedicated news and news analysis. Indeed, the timeliness of delivery always takes precedence over the depth of analysis or accuracy of the material.

This is a by-product of a commercial market dynamic, in which competing media players must attract the interest of viewers to achieve favourable ratings and thus attract subscriptions or advertising revenues. In a sense this is a commercial application of Goebbels' dictum that 'propaganda must be entertaining', the aim of this propaganda being transmission of the message that 'this media organisation is more attractive than its competitors' (Goebbels, 1943).

The empirically observable reality is that viewers and readers are most attracted to footage or stories which are dramatic, violent or involve intense controversy. Another empirically observable reality is that media organisations will aim to appeal to existing prejudices or preconceptions on the part of the audience. The latter is the same mechanism observed in propaganda distribution, as presentation of materials which challenge audience prejudices or preconceptions will be less likely to be received favourably, and thus damage the commercial yield of the organisation – or propaganda effect of a regime targeting its population.

In terms of the canonical Information Warfare strategies, the play by media organisations is a compound strategy of degradation and corruption, centred on audience interest and apriori prejudices and aimed at maximising audience visitation rates at the expense of competitors. It is effectively a competitive game of 'who has the best honeypot?' with the game payoff in the frequency of visitation.

A regime or political movement intending to target an audience on the global stage, especially the populations of Western democracies, can only be successful if it can wrap its deceptive message in an envelope of material which is attractive to global media organisations. As a result the deceptive message must provide content which is dramatic, violent, intensely controversial, or any combination of the three, and which appeals to the prejudices of the target population in the deception game.

At the most fundamental level of the four strategies of Information Warfare, regimes or political movements targeting Western or global populations with deceptive propaganda and using the global mass media as a conduit, employ compound strategies combining denial through subversion, degradation and corruption strategies. Denial via destruction of the delivery channel is usually avoided since it compromises the intermediate aim of the strategy, which is exploitation of the delivery channel.

There are two notable examples of this model being used. The first is the play by North Vietnam against the United States and its allies during the South East Asian conflict, where mass media were used as a conduit to deliver deceptive propaganda to the global, and especially US populations. This campaign was successful as media self interest enabled its use a high volume conduit to effect a denial via subversion strategy. US consumers via advertising revenue to media funded the distribution of deceptive propaganda which destroyed public support for the war and led to a US withdrawal.

The more recent example is the ongoing campaign of kidnappings, suicide bombings, roadside bombings and assassinations in Muslim nations, the recent public transport bombings in Spain and the UK, and the September 11 attacks in the US. No differently than during the South East Asian conflict, global consumers are funding the distribution of deceptive propaganda via media organisations.

The dominant deception technique used in both campaigns is the Lure, which is employed to facilitate distribution of deceptive messages via mass media channels.

This play is currently implemented by providing spectacular acts of violence, which are employed to compel mass media distribution and thus subsequent uptake by the target populations. The deceptive messages which target the victim population include 'we have the power to hurt you', 'we are a ferocious opponent', 'you can never defeat us' and 'your government cannot protect you from us'. The aim is to destroy the population's confidence in its leadership and to elicit disproportionate military responses which can be used to reinforce deceptive propaganda distributed in Muslim nations.

It is interesting to observe that the Soviet regime was more sophisticated in many of its deception techniques targeting Western populations and using the media as a conduit. Techniques such as the Unintentional Mistake and Piece of Bad Luck were used repeatedly to distribute fabricated US or NATO military documents to media organisations with known pro Soviet bias.

CONCLUSIONS

The classical deception techniques can be readily remapped into canonical forms based on the four fundamental strategies of Information Warfare. Most frequently these forms involve compound strategies, especially using combinations of degradation and corruption of information. In some situations these games also include a denial through subversion component, in which the victim's resources are used to inflict damage.

Established mass media perception management techniques can be divided into two categories, each targeting distinct victim populations.

The techniques most frequently employed by authoritarian regimes or movements which control media content yield a one to one mapping to the classical deception techniques and supporting methodology, and thus represent a hypergame in which the regime and the victim population are mutual opponents.

Techniques used by such regimes or movements to attack the global community via mass media channels are invariably compound strategies, centred on a denial through subversion play against the victim population, in which degradation and corruption are used to facilitate mass media distribution of the deceptive message.

REFERENCES

- 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].
- Fischer B.B. (1999) Stalin's Killing Field, The Katyn Controversy, *Studies in Intelligence, Journal of the American Intelligence Professional*, Winter 1999-2000, URL: <http://www.cia.gov/csi/studies/winter99-00/art6.html> [Date accessed 20/10/2005].
- Fraser N. M., Hipel K. W. (1984), *Conflict Analysis, Models and Resolution*. North-Holland, Elsevier Science Publishing Co., New York, USA.
- Goebbels J. (1943) *Der treue Helfer, Das eherne Herz* (Munich: Zentralverlag der NSDAP, 1943), pp. 229-235, translated as 'The Good Companion', German Propaganda Archive, URL: <http://www.calvin.edu/academic/cas/gpa/goeb12.htm> [Date Accessed 20/10/2005].
- Goebbels J. (1938) *Der Rundfunk als achte Grossmacht, Signale der neuen Zeit. 25 ausgewahlte Reden von Dr. Joseph Goebbels* (Munich: Zentralverlag der NSDAP., 1938), pp. 197-207, translated as 'The Radio as the Eighth Great Power', German Propaganda Archive, URL: <http://www.calvin.edu/academic/cas/gpa/goeb56.htm> [Date Accessed 20/10/2005].
- Goebbels J. (1934) *Der Kongress zur Nuernberg 1934* (Munich: Zentralverlag der NSDAP., Frz. Eher Nachf., 1934), pp. 130-141, translated as 'Goebbels at Nuremberg - 1934', German Propaganda Archive, URL: <http://www.calvin.edu/academic/cas/gpa/goeb59.htm> [Date Accessed 20/10/2005].
- Goebbels J. (1944) *Nun, Volk steh auf, und Sturm brich los! Rede im Berliner Sportpalast, Der steile Aufstieg* (Munich: Zentralverlag der NSDAP, 1944), pp. 167-204, translated as 'Nation, Rise Up, and Let the Storm Break Loose', German Propaganda Archive, URL: <http://www.calvin.edu/academic/cas/gpa/goeb36.htm>

[Date Accessed 20/10/2005].

- Goebbels J. (1940) Die Zeit ohne Beispiel, Das Reich, 23 May 1940, pp. 1, 3, translated as 'A Unique Age', German Propaganda Archive, URL: <http://www.calvin.edu/academic/cas/gpa/goeb70.htm> [Date Accessed 20/10/2005].
- Goebbels J. (1944) Das hoehere Gesetz, Das Reich, 24 September 1944, pp. 1, 3, translated as 'The Higher Law', German Propaganda Archive, URL: <http://www.calvin.edu/academic/cas/gpa/goeb65.htm> [Date Accessed 20/10/2005].
- Grabo C.M. (2000) Soviet Deception in the Czechoslovak Crisis, Studies in Intelligence, *Journal of the American Intelligence Professional*, Special Unclassified Edition, Fall 2000, URL: http://www.cia.gov/csi/studies/fall00/ch5_Soviet_Deception.pdf [Date accessed 20/10/2005].
- Hansen J. H. (2002) Soviet Deception in the Cuban Missile Crisis, Learning from the Past, Studies in Intelligence, *Journal of the American Intelligence Professional*, Vol. 46, No. 1, 2002, Unclassified Edition, URL: <http://www.cia.gov/csi/studies/vol46no1/article06.html> [Date accessed 20/10/2005].
- Haswell J. (1985) *The Tangled Web: The Art of Tactical and Strategic Deception*. Wendover, John Goodchild, 1985.
- Holland M. (2001) The Lie That Linked CIA to the Kennedy Assassination, The Power of Disinformation, Studies in Intelligence, *Journal of the American Intelligence Professional*, Fall-Winter 2001, No. 11, Unclassified Edition, URL: http://www.cia.gov/csi/studies/fall_winter_2001/article02.html [Date accessed 20/10/2005].
- Kerbel J. (2004) Thinking Straight: Cognitive Bias in the US Debate about China, Rethinking Thinking, Studies in Intelligence, *Journal of the American Intelligence Professional*, Vol. 48, No. 3, 2004, Unclassified Edition, URL: <http://www.cia.gov/csi/studies/vol48no3/article03.html> [Date accessed 20/10/2005].
- Kern G. (2003) How 'Uncle Joe' Bugged FDR, The Lessons of History, Studies in Intelligence, *Journal of the American Intelligence Professional*, Vol. 47, No. 1, 2003, Unclassified Edition, URL: <http://www.cia.gov/csi/studies/vol47no1/article02.html> [Date accessed 20/10/2005].
- 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.
- Kopp C., (2005) The Analysis of Compound Information Warfare Strategies, *Proceedings of the 6th Australian Information Warfare Conference*, Deakin University, Geelong. November, 2005.
- Mendez A.J. (1999) A Classic Case of Deception, Studies in Intelligence, *Journal of the American Intelligence Professional*, Winter 1999-2000, URL: <http://www.cia.gov/csi/studies/winter99-00/art1.html> [Date accessed 20/10/2005].
- Widnall S. E., Fogelman R. R. (1997), *Cornerstones of Information Warfare*. Doctrine/Policy Document, United States Air Force.

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.