4-12-2006

Considerations on Deception Techniques Used in Political and Product Marketing

Carlo Kopp
Monash University

DOI: 10.4225/75/57a80fdfaa0cc
7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

Considerations on Deception Techniques Used in Political and Product Marketing

Carlo Kopp
carlo@cs.monash.edu.au
Clayton School of IT
Monash University
Melbourne, Australia

Abstract

This paper explores three deception techniques which are widely used in political and product marketing. These techniques are 'deception by omission', 'deception by saturation' and the use of 'deception by spin'. These techniques are newly analysed in the framework of the four canonical strategies of Information Warfare and Shannon's capacity and entropy theorems, and their respective strengths and weaknesses established. Specific strategies for the defeat of these deception techniques are discussed.

Keywords

Deception, Marketing, Propaganda, Spin, Omission, Saturation, Information Warfare

INTRODUCTION

Instances of deception in political and commercial product marketing are well documented and historically well established, but to date have never been analysed in the framework of the four canonical strategies, in any detail. Therefore no basis has existed for formally modeling these techniques in a mathematically supportable form (Alterman, 2005; Kahn, 2006; Delamarter, 1986; Hagley, 2006).

The aim of this paper is scientific, and centered in the application of information theory. The paper is intended to newly map the three deception techniques used most frequently in political and commercial product marketing into models based upon the four canonical strategies of Information Warfare, and explore their characteristics from the perspective of the four canonical strategies. The focus of this paper is on the mapping of these techniques. It is not intended to survey deceptive political and commercial product marketing case studies, or explore or comment on the history, motivation or ethics of such deceptions. Examples chosen have been done so as they are well documented and provide clear instances of such deceptions. Some brief examples and case studies are used to illustrate these deception techniques for readers who may lack a background in the mathematics of information theory, specifically Shannon's capacity and entropy theorems (Shannon, 1948).

This paper, by mapping techniques used in political and commercial product marketing into the four canonical strategies, completes a body of work which has aimed to map all commonly arising deception techniques into the four canonical strategies (Kopp 2003, 2005A, 2005B; Kopp and Mills, 2002).

The 'classical' theory of deception mostly predates the formal mathematical formulation of the theory of Information Warfare. It has been recently mapped into the four canonical strategies (Borden, 1999; Kopp, 2000; Kopp, 2005B). This mapping shows that the dominant technique used in military and strategic deceptions, and propaganda deceptions where the attacker unilaterally controls the medium used for information distribution, is a *Corruption/Mimicry* strategy, usually supported by *Degradation/Denial* strategy.

Definition: For the purpose of this paper, commercial product marketing is defined as the presentation of information pertaining to products which is intended to compel a potential customer to select these products over competing products. Deception in commercial product marketing is defined as the use of deception techniques to achieve the aim of marketing the commercial product despite the limitations or unwanted characteristics of the product in the perception of the potential customer.

Definition: Political marketing, for the purpose of this paper, is defined as the presentation of information pertaining to policy decisions or actions by a political or government entity which is intended to compel the population, the legislature or an organization to consent to a policy decision or action, despite the limitations or unwanted characteristics of the policy decision or action in the perception of the population, the legislature or the organization. Deception in political marketing is defined as the use of deception techniques to achieve the aim of marketing policy decisions or actions despite the limitations or unwanted characteristics of these in the perception of the population, the legislature or the organization.

Deception techniques demonstrably qualify as a biological survival mechanism (Kopp, Mills, 2002), evolved specifically for the purpose of gaining an advantage in a survival game. If we consider political or commercial product marketing as a competitive survival game between players, then this biological model maps directly into the behaviours seen in marketing, where deception is used to aid survival in this instance of commercial or political entities.

In mathematical terms, deception techniques are 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. 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.

Definition: The four canonical strategies of Information Warfare are defined thus (Kopp, 2003; 2006):

> **Degradation or Destruction [also Denial of Information]**, that is 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. We can further divide degradation attacks into 'active' and 'passive', depending on whether the attacker generates the signal, or hides the signal.
> **Corruption [also Deception and Mimicry]**, that is the insertion of intentionally misleading information; corruption amounts to mimicking a known signal so well, that a receiver cannot distinguish the deceptive signal from the real signal.
> **Denial [also Disruption and Destruction],** that is 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.
> **Denial [also Subversion]** , that is 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.

These definitions are included for the benefit of readers who do not have prior familiarity with the four canonical strategies.

DECEPTION IN POLITICAL AND PRODUCT MARKETING

As numerous examples over many centuries illustrate, the full spectrum of deception techniques has been used to promote political agendas and to market products. The use of such techniques however became most prominent during the twentieth century, with the advent of mass media as a distribution channel (Alterman, 2005; Kahn, 2006; Delamarter, 1986, Volpe, 1978; Beasey, 1973).

At the fundamental level deception techniques used for these purposes are designed to function within a specific type of environment, within the constraints imposed by that environment. As noted previously, propaganda and media deception techniques used in situations where the distribution channel can be controlled characteristically map into Corruption/Mimicry strategies, most often supported by Degradation/Denial strategies, thus forming compound strategies (Kopp, 2005A; 2005B).

Analysis of numerous case studies indicates that 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 (Haswell, 1985). Instances of intelligence and internal propaganda deceptions are well detailed in (Holland, 2001), (Fischer, 1999), (Grabo, 2000) and (Goebbels, 1934; 1938; 1940; 1943; 1944; 1944).

A prerequisite for the use of these techniques is that no or very few constraints exist upon the control of the distribution channel. Typically, two scenarios exist for control of a distribution channel. The first is where the channel is operated by the apparatus of state, the second is where the channel may be operated by a third party, but the propaganda message is attractive for other reasons to the operator of the channel, who is prepared to become a proxy for the attacker to otherwise benefit from the attack (Kopp, 2005A; 2005B).

More generally, control of the channel and unconstrained choices in the use of Corruption/Mimicry strategies cannot be assumed, especially where legislation or ownership impose hard limits on how the channel can be employed, and what types of messages can be transmitted.

In most developed nations untruthful statements, or application of a *Corruption/Mimicry* strategy in political or product marketing are unlawful or present grounds for civil action. In Australia most such offences fall under Section 52(1) of the Trade Practices Act 1974 Commonwealth, which prohibits engagement in *conduct that is misleading or deceptive, or is likely to mislead or deceive* (ABS, 2006; ALII,2006). Therefore deception techniques which avoid explicitly untruthful statements may be the only legally safe deception technique available, and thus the only techniques which may be safely utilized by an attacker.

In Western democracies with active media, it is frequently difficult to impose control on the flow of information or to effectively propagate deceptions which are easily proven to be such. Thus the most common deception techniques employed are *Deception by Omission*, *Deception by Saturation* and *Deception by Spin* (Kopp, 2006).

All of these techniques are designed to create a misperception of reality by either excluding unpalatable facts, or encouraging the victim to devalue or disregard unpalatable facts by accepting the 'spin' on the issue.

DECEPTION BY OMISSION

Deception by Omission is a form of Passive Degradation, the first canonical strategy. The attacker hides information which would be unhelpful or deleterious in driving the victim of the deception to a specific misperception of reality (Kopp, 2006).

In terms of Shannon's model for channel capacity (Shannon, 1948):

$$C = W \log_2 (1 + \frac{P}{N})$$

Where C is capacity, W bandwidth, P message or signal power, and N noise power, the unwanted message is omitted and thus P→0 for unwanted information, reducing its contribution to channel capacity to zero.

Two assumptions are made in this model. The first is that the victim receiver can wholly understand and thus decode the messages it receives, which may or may not be true in the general case. The second is that some repeatable mapping exists between a message, background noise and the quantitative measures of P and N. This paper does not aim to determine that mapping in the general case.

A basis for establishing such a mapping will lie in Shannon's entropy theorem, which shows that a message with an entirely predictable content has no information content (Shannon, 1948):

$$I(m) = -\log_2 (p(m))$$

Where $I(m)$ is the information content of the message, and $p(m)$ the probability of the message arising. If $p(m) \rightarrow 1$, inevitably $I(m) \rightarrow 0$, that is messages which are certain to arise tell the receiver nothing. If we define noise in this channel as being those messages without useful content, from the receiver's perspective, then a basis exists for determining a mapping.

A prerequisite for *Deception by Omission* is that the victim has poor *a priori* knowledge or no *a priori* knowledge or understanding of what the attacker is presenting to be a picture of reality. A misperception of reality favourable to the attacker can be implanted if the victim can be induced to form a picture of reality based only upon what the attacker presents. Hiding the existence of unwanted facts which interfere with the formation of a desired picture of reality in the mind of the victim may or may not be easy to implement. Pertinent examples in the political domain would include instances of adverse policy outcomes, adverse studies or reports on policy outcomes, present or future, being suppressed or not disclosed to the public. In the marketing of commercial products for consumers, or industrial clients, concealment is characteristically implemented by not disclosing known problems or limitations in products, or adverse side effects the products may produce when used.

The best defence a potential victim of a Deception by Omission attack has is to ensure that multiple independent channels are used to collect information. In this fashion outputs from multiple channels can be compared. Where differences arise, these can be analysed to establish what information may have been omitted.

Deception by omission is a very popular technique in commercial product marketing and political marketing since it permits attacks without resorting to making provably untruthful statements, that is Corruption. Over recent decades regulatory or legislative measures have been adopted in most developed nations to force disclosure of factual information on products or compliance with specific regulations or law. Nevertheless the deception by omission technique is often successful due to laziness or incompetence on the part of a victim population.

The first case study draws upon public evidence provided by the Australian Department of Defence to the Canberra Joint Standing Committee on Foreign Affairs, Defence and Trade as part of the Defence Annual Review of 2002-2003, and is an instance of political deception (FADT, 2004).

The background to this evidence is that in 2003 the Australian Department of Defence opted to arbitrarily retire the Australian F-111 strike fighter fleet a decade earlier than planned for, having previously decided in 2002 to acquire the Joint Strike Fighter as Australia's future combat aircraft. In the context of Australian military planning, historically such decisions were made on the basis of extensive analysis and study. Both the F-111 and Joint Strike Fighter decisions were made without prior analytical study, which resulted in intensive public criticism of both decisions. In response to this criticism, the Australian Department of Defence made a wide range of public statements and provided evidence to the Joint Standing Committee on Foreign Affairs, Defence and Trade.

Elements of that evidence present excellent examples of *Deception by Omission, Deception by Saturation* and *Deception by Spin*, directed at the Committee, the Australian public, with the political aim of avoiding parliamentary and public censure, and the Australian Department of Defence itself, the latter with the aim of maintaining internal cohesion (FADT, 2003). While a study of deception objectives and self deception is not an aim of this paper, this example presents an interesting case study insofar as the organization was effectively damaging its own capability and credibility by pursuing this chosen course of action (Brumley, 2006).

Deception by Omission arises frequently. Repeated instances include:

1. Avoidance of any discussion of material risks arising in the Joint Strike Fighter program, despite these attracting a large volume of press globally (FADT, 2003).
2. Avoidance of any detailed discussion of the capabilities of the competing F-22 fighter, despite this information being widely available in the public domain (FADT, 2003).
3. Avoidance of any discussion of the adverse consequences of early retirement of the F-111 aircraft, despite these being extensively documented in the public domain (FADT, 2003).

4. Avoidance of any discussion of the capabilities of competing foreign aircraft being acquired across the region and presenting a challenge to the Joint Strike Fighter, thus concealing its weaknesses (FADT, 2003).

Case studies of *Deception by Omission* in the commercial domain are also abundant. A good summary of examples in the computer industry can be found in DeLamarter's work, which presents and distills evidence compiled during the US Justice Department anti-trust suit against IBM (Delamarter, 1986; Hagley, 2006). *Deception by Omission* arises frequently, primarily in instances where adverse limitations of vendor equipment, or impending unavailability of products are not disclosed to the customer. This technique has become widely adopted across the computer industry, in this author's prior experience as a Chief Engineer, and is not unique to IBM practice of that period.

A problem arising for attackers who repeatedly play a *Deception by Omission* strategy is that the victim population will over time learn that this strategy is being played, and as a result become mistrustful of the attacker. Nevertheless the *Deception by Omission* strategy remains widely used as the victim population is often unwilling to invest the effort required to defend itself, especially in the procurement of commercially marketed products.

DECEPTION BY SATURATION

Deception by Saturation arises in two forms, either as an *Active Degradation* attack, or a *soft kill Denial by Destruction* attack. In executing a *Deception by Saturation* attack, the attacker will inundate the victim with messages, most of which are redundant or irrelevant, with the aim of saturating the victim's channel so the victim cannot gather information which might contradict the attacker's message. Even an alert victim who may have the capacity to find valid messages embedded in a large volume of redundant messages may be effectively attacked, if the victim does not have the available time to sort through all of the received messages.

As an *Active Degradation* attack, *Deception by Saturation* aims to hide unwanted information behind a deluge of messages which have little or no information content. This technique is distinct from *Deception by Omission* as it involves the active generation of messages with deceptive intent, whereas the former involves the omission of messages, doing so with deceptive intent.

As stated earlier, Shannon's entropy theorem shows that a message with an entirely predictable content has no information content. Given $I(m)$ is the information content of the message, and $p(m)$ the probability of the message arising, then where $p(m) \rightarrow 1$, inevitably $I(m) \rightarrow 0$, that is messages which are certain to arise tell the receiver nothing.

In effect the messages used to implement the attack can be considered to be noise in the channel, devoid of information content. Where the victim cannot successfully filter a message from the background noise, for whatever reason, the capacity of the channel will degrade down to zero. In terms of Shannon's model for channel capacity (previously cited), the redundant or information free messages represent noise N and thus $N >> P$ resulting in $C \rightarrow 0$.

In the context of *Deception by Saturation* attacks, attacks in which the victim has the opportunity to receive and decode every message in the channel, be they deceptive or real messages, must be classed as *Active Degradation* attacks not unlike jamming of radiofrequency communications channels. In such attacks the attacker is successful where the limitations of the victim's receiver prevent the victim from separating real messages from messages produced by the saturation attack.

The alternate form of this attack is one in which the victim does have the capability to distinguish the real message from the redundant or information free messages but is unable to perform this operation in reasonable time and thus fails to distinguish between the attacker's message and the real message.

In terms of Shannon's model for channel capacity this is a situation where the bandwidth of the channel is inadequate to the problem, that is $W << W_{required}$. As a result the capacity available is not enough to carry the real message and the attack succeeds. Attacks which compromise the available channel bandwidth rendering it unusable are classified as soft kill *Denial by Destruction* attacks.

Deception by Saturation remains widely used in marketing of commercial and political products, primarily as much of the victim population is unable or unwilling to invest the effort required to filter redundant or information free messages from real messages. It is worth observing that trivial strategies for analysing the veracity of messages, based on assumptions such as 'messages which are more numerous must be somehow more truthful' provide attractive opportunities for attackers using this technique.

A good case study exists in the previously cited evidence presented to the Canberra Joint Standing Committee on Foreign Affairs, Defence and Trade. Repeated instances include:

1. Superficial but lengthy descriptions of the desirable attributes of the Joint Strike Fighter, none of which introduce any new information content (FADT, 2003; 2004).
2. Superficial but lengthy descriptions of the undesirable attributes, limitations or failings of the F-111, devoid of actual substantiation (FADT, 2003; 2004).

Both of these examples are characterized by often very long discussions of the issue in question, using verbose language and often unnecessary technical jargon, introduced in the knowledge that the target audience will need to expend time in referencing the language and understanding the terms used, thus effecting a soft kill *Denial by Destruction* attack.

This is a well crafted *Deception by Saturation* strategy, insofar as legislators, who were the primary targets of these attacks, are more than often constrained in the time they have available for hearings, meetings and reading of evidence. Since few legislators have the background knowledge and understanding required to rapidly filter actual information content from the *Deception by Saturation* attack conducted in such a specialised area of debate, the use of this strategy can be highly profitable. This also explains why this technique is commonly used in bureaucratic deceptions aimed at legislators (FADT, 2006B).

A good summary of examples in the commercial domain can be found in the previously cited work by DeLamarter, on the US Justice Department anti-trust suit against IBM (Delamarter, 1986; Hagley, 2006).

Deception by Saturation is frequently used, and best represented by large volumes of marketing literature and brochures which contain little actual technical content. The audience is presented thus with the task of sifting through large volumes of material to extract a small volume of technical content which is actually required to make a rational procurement decision, and constitutes information content in the sense of the entropy theorem. This practice is also not unique to IBM during that period, in this author's prior industry experience.

This technique is not covered by regulation or legislation. In commercial tendering, bid size limiting has been used as an effective defence mechanism. By constraining the size of tender proposal documents, the victim (client) can force the attacker (bidder) to maximise the ratio of P to N, within a constrained W.

In the most general sense, if a victim expects to be subjected to this regime of attack, prudent planning sees sufficient resources allocated *a priori* to ensure that all messages can be read and understood properly in reasonable time. This permits messages which are devoid of information content to be filtered and discarded.

DECEPTION BY SPIN

Deception by Spin is a form of *Subversion* attack, and is often used in a compound strategy supported by *Deception By Omission*, or sometimes *Deception By Saturation*. A spin attack is based on the idea of presenting an unpalatable or other acknowledged or accepted fact, but encouraging the victim to assess that fact from a perspective which is less damaging to the attacker. The victim's mechanism for critically assessing the unpalatable fact is thus subverted. Other than this basic form of attack, an alternate form where the unwanted reality is not connected with the victim's assessment is also used. This designate the latter as an *Indirect Deception by Spin.*

A trivial example of the basic form might be thus – "here is an fact which is true, but it isn't really that bad because of the following circumstances ….", in which the explanation of 'following circumstances' compels the victim to devalue the unwanted consequences of the unpalatable fact. The attacker presents 'following circumstances' which may in themselves not be untruthful, but achieve a deceptive aim by altering the victim's interpretation of the message to the advantage of the attacker.

It is worth observing that a well executed spin attack is typically a compound strategy, in which the absence of evidently untruthful message content amounts to the use of a supporting *Corruption* strategy to insert the *Subversion* into the victim's mind. Spin attacks, like deception by omission attacks, rely on the victim having little or no *a priori* knowledge or understanding, and the victim not being prepared to critically analyse a statement by the attacker. The use of spin attacks thus often relies on the trust of the victim, or victims who are fearful of losing confidence in the attacker.

In information theoretical and information processing terms, *Deception by Spin* is a classical compound *Subversion* attack which is targeted against the interpretation phase of the *Orientation* step in the victim's *Observation Orientation Decision Action* loop. As the victim uses its own internal processing resources to infer false conclusions from the received message, the victim has been effectively subverted to an internal state which is intended by the attacker (Brumley et al, 2006).

The most effective defence against basic spin attacks is to explore what is being presented as the 'it is not so bad' qualification or 'following circumstances' to find what adverse consequences may have been excluded, concealed or otherwise deceptively denied to the victim. This defensive play will however require investment of some effort to implement, and often such effort may be infeasible given available resources.

Spin attacks have been used widely in the political debate, but are also increasingly a feature of other public debates, notably on environmental issues and consumer products. Mostly spin attacks are used where some adverse reality which cannot be concealed by the attacker must be dealt with. Spin attacks can be highly effective where the victim is not prepared to apply critical thought to analysing attackers' messages. Spin attacks are not covered by legislation or regulation, and unless supported by an explicit Corruption strategy, remain legal. As a well crafted spin attack may comprise components which are all truthful in themselves, the attacker can defend the use of the spin attack as not being deceptive when challenged.

A good case study exists in the previously cited evidence presented to the Canberra Joint Standing Committee on Foreign Affairs, Defence and Trade. Instances of *Deception by Spin* are less frequent than *Deception by Omission* and *Deception by Saturation* in this case study, most likely due to the additional effort required to produce such a deception. Prominent instances include:

1. Repeated admissions of F-111 groundings due to faults and failures, which are consistently explained as 'age related'. As detailed analysis of each instance shows these were the result of poor engineering or planning, rather than age. The argument that age is the cause was intended to shift the manner in which the audience interprets the admitted failures to shift responsibility away from poor engineering or planning practices, and thus represents an excellent example of spin technique (FADT,2003).
2. The applicability of 'throw weight', a generalized measure of strike force potency, is explained to be irrelevant for a variety of reasons, none of which are actually pertinent to the argument. This was intended to compel the audience to devalue the negative conclusions of a 'throw weight' analysis of the Defence position (FADT, 2003; 2004).
3. The inability of the Joint Strike Fighter to compete with the larger F-111 in bomb carriage capabilities is explained to be irrelevant as future bombs will be smaller and lighter. As bomber potency scales with the number of smart bombs carried, this argument is intended to deceptively lead the audience to disregard the actual limitations of Joint Strike Fighter and is thus a spin attack (FADT,2003).
4. Projections of increased future F-111 operating costs, using irrelevant models and examples which do not fit the maintenance regime incurring these costs. The models and examples are used to compel the audience to disregard the reasons why these projections overstate the actual cost (FADT,2003).

The repeated and consistent use of techniques based upon *Deception by Spin*, *Deception by Omission* and *Deception by Saturation* appears to be a feature of how the Australian Department of Defence produces many of its documents and statements to the public and the parliament. All three techniques have been used repeatedly in subsequent evidence and submissions (FADT, 2006A; 2006B).

In the commercial domain, well documented examples can be found in DeLamarter's work. *Deception by Spin* is less frequent than deception by the previous tow techniques. The best single case study is the widely used practice of stimulating *Fear Uncertainty and Doubt (FUD*) in customers. The unwanted (by the attacker) impact of a competing product is explained in terms of the competing product introducing risks to the customer's operation, and thus not presenting a credible alternative. This is a spin attack, insofar as the acknowledged reality of a competing product is presented to be irrelevant for reasons which are essentially speculative, but play on the victim's anxieties (Delamarter, 1986).

Another rich and well documented source of case studies of *Deception by Spin* exists in the history of the public relations industry (MPRW, 2006).

A good example is the 1934 'Green Ball' campaign by Edward L. Bernays, who confronted with public rejection of green coloured Lucky Strike cigarette packaging, sought to alter public views on the attractiveness of green colouring by launching a prestigious charity ball at which all gowns worn were required to be green in colour. This is a highly refined spin attack, in that the attacker's agenda is wholly hidden (MPRW, 2006A).

Bernays later repeated this type of spin attack during the Philco Radio campaign, where a lack of affluent consumer market penetration by radio receiver products was countered by the launching of a gala black tie event at a prestigious Rockefeller Plaza gallery in New York (MPRW, 2006B).

Bernays pioneered the *Indirect Deception by Spin* attack, using the idea of separating the *Subversion* attack proper from the adverse reality which the attacker is aiming to dispel, thus making defence against the spin attack difficult to achieve. Unless the victim is in the position to backtrack the funding trail behind the public relations campaign, it will be especially difficult to establish that a spin attack is in progress. This technique avoids the weakness in most common spin attacks, where the adverse reality is visibly connected with the argument as to why it is not important.

It is reasonable to expect that spin attacks will increase in use over time as they are easily defended when challenged. Unless legislation is introduced which legally defines spin attacks and makes them unlawful, their use will remain attractive to potential attackers.

CONCLUSIONS

This paper has analysed mass media political and commercial marketing deceptions used in developed nations in the framework of the four canonical strategies of Information Warfare and Shannon's capacity and entropy theorems. These deceptions are characterised by the wide use of three techniques, *Deception by Omission, Deception by Saturation* and *Deception by Spin*, usually employed as part of compound strategies.

The key feature of all three strategies at the level of the canonical IW strategies is that all three of these techniques avoid the explicit use of the *Corruption* strategy, as it is often legislated against.

This paper has shown that *Deception by Omission* is a form of passive *Degradation* attack, the first canonical strategy, and provides an original explanation of this in terms of Shannon's capacity theorem .It has shown that *Deception by Saturation* arises in two forms, the first as an *Active Degradation* attack*,* the second as a *soft kill Denial by Destruction* attack. Both forms are explained in terms of Shannon's capacity and entropy theorems, an analysis unique to this paper. It has also shown that *Deception by Spin* is a form of *Subversion* attack, and explained its relationship to supporting strategies, and the Orientation step of Boyd's OODA loop, not analysed in previous publications. Defensive techniques exist for all three of these strategies, but require preparation and investment of resources or time on the part of a potential victim of such an attack.

Opportunities will exist for further research in relating in more detail these techniques to component phases of the Orientation step in Boyd's OODA loop, and in the refinement of defensive strategies. Statistical analysis of case studies to determine frequencies of specific deception techniques could also be performed to determine where effort in defensive technique should be best invested. Another area of productive future research will be in further exploration of the relationship between message content and Shannon information.

REFERENCES

ABS (2006), 1234.0 - Australian Standard Offence Classification (ASOC), 1997, Deception and Related Offences, Australian Bureau of Statistics, URL: http://www.abs.gov.au/ausstats/abs@.nsf/66f306f503e529a5ca25697e0017661f/F05019D51C545B39CA25697E00184AE7?opendocument [Date Accessed 09/11/2006].

ALII (2006), TRADE PRACTICES ACT 1974 - SECT 52, Australasian Legal Information Institute, Commonwealth Consolidated Acts, URL: http://www.austlii.edu.au/au/legis/cth/consol_act/tpa1974149/s52.html [Date Accessed 09/11/2006].

Alterman E (2005), *When Presidents Lie - A History of Official Deception and Its Consequences*, Penguin Group, URL: http://us.penguingroup.com/nf/Book/BookDisplay/0,,9780786552771,00.html [Date accessed: 01/09/04].

Beasey, M F (1973), It's What You Don't Say: *Omissio* in Cicero's Speeches, *Southern Speech Communication Journal* 39: 11-20.

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].

Brumley L, Kopp C, Korb K (2006), Causes and Effects of Perception Errors, *Journal of Information Warfare*, Edith Cowan University, Perth, WA, Australia, ISSN: 1445-3312, Vol 5, Issue 3, pp 41-53.

DeLamarter R (1986), *Big Blue: IBM's Use and Abuse of Power*, New York: Dodd, Mead & Company.

FADT (2003), Official Committee Hansard, *Review of Defence Annual Report 2002-03*, Monday, 15 December 2003, Canberra, URL: http://www.aph.gov.au/hansard/joint/commttee/J7170.pdf [Date Accessed 09/11/2006].

FADT (2004), Submissions, *Review of the Defence Annual Report 2002-2003*, Joint Standing Committee on Foreign Affairs, Defence and Trade, Parliament of Australia, URL: http://www.aph.gov.au/house/committee/jfadt/defenceannualreport_2002_2003/dar_subs.htm [Date Accessed 09/11/2006].

FADT (2006A), Submissions, *Inquiry into Australian Defence Force Regional Air Superiority*, Joint Standing Committee on Foreign Affairs, Defence and Trade, Parliament of Australia, URL: http://www.aph.gov.au/house/committee/jfadt/adfair/subs.htm [Date Accessed 09/11/2006].

FADT (2006B), Submissions, *Inquiry into Australia's regional strategic defence requirements*, Joint Standing Committee on Foreign Affairs, Defence and Trade, Parliament of Australia, URL: http://www.aph.gov.au/house/committee/jfadt/esstrends/subs.htm [Date Accessed 09/11/2006].

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].

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 ausgewaehlte 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].

Hagley (2006), *IBM Antitrust Suit Records 1950-1982*, website archive, Hagley Museum and Library, Wilmington, DE 19807-0630, URL: http://www.hagley.lib.de.us/1980.htm [Date Accessed 09/11/2006].

Kahn V. (2006), *Machiavellian Rhetoric:From the Counter-Reformation to Milton*, (e-Book) Princeton University Press, URL: **http://press.princeton.edu/titles/5480.html** [Date Accessed 09/11/2006].

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 (2005A), *The Analysis of Compound Information Warfare Strategies*, in G Pye and M Warren (eds), Conference Proceedings of the 6th Australian Information Warfare & Security Conference (IWAR 2005), Geelong, VIC, Australia, School of Information Systems, Deakin University, Geelong, VIC, Australia, ISBN: 1 74156 028 4, pp 90-97.

Kopp C (2005B), *Classical Deception Techniques and Perception Management vs. the Four Strategies of Information Warfare*, in G Pye and M Warren (eds), Conference Proceedings of the 6th Australian Information Warfare & Security Conference (IWAR 2005), Geelong, VIC, Australia, School of Information Systems, Deakin University, Geelong, VIC, Australia, ISBN: 1 74156 028 4, pp 81-89.

Kopp C, (2006) *CSE 468 Information Conflict*, Lecture Notes, Clayton School of Information Technology, Monash University, URL: http://www.csse.monash.edu.au/courseware/cse468/subject-info.html [Date Accessed 03/05/2006].

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].

MPRW (2006), *The Museum of Public Relations*, website, 65 Broadway / Suite 820 New York, NY 10006, URL: http://www.prmuseum.com/welcome.html [Date Accessed 09/11/2006].

MPRW (2006A), 1934 – The Green Ball, *The Museum of Public Relations*, website, 65 Broadway / Suite 820 New York, NY 10006, URL: http://www.prmuseum.com/bernays/bernays_1934.html [Date Accessed 09/11/2006].

MPRW (2006B), 1939 – Philco Radio and Television, *The Museum of Public Relations*, website, 65 Broadway / Suite 820 New York, NY 10006, URL: http://www.prmuseum.com/bernays/bernays_1939.html [Date Accessed 09/11/2006].

Shannon C.E. (1948), A mathematical theory of communication, *Bell System Technical Journal,* vol. 27, pp. 379-423 and 623-656, July and October, 1948. URL: http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html [Date Accessed 03/05/2006].

Volpe M (1978), Cicero's Dust: Deception, Diversion or Different Perspective?, *Communication Studies* 29: 118–126.

COPYRIGHT