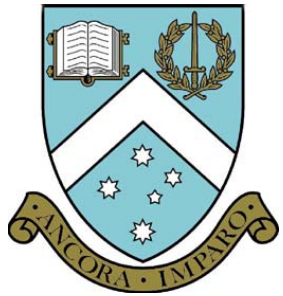


Considerations on Deception Techniques Used in Political and Product Marketing

Dr Carlo Kopp, MIEEE, MAIAA, PEng
carlo@csse.monash.edu.au
Clayton School of Information Technology
Monash University, Clayton 3800, 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.

The Four Canonical Strategies of InfoWar

- **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.
- **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 phoney signal from the real signal.
- **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.
- **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.

Classical Theory of Deception

- 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 .
- 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 - Commercial Product Marketing

- 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

- Political marketing 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.

The Channel – Controlled or Uncontrolled?

- Generally, control of the channel and unconstrained choices in the use of *Corruption/Mimicry* strategies cannot be assumed.
- Where legislation or ownership impose hard limits on how the channel can be employed, and what types of messages can be transmitted, control cannot be assumed.
- In Western democracies with active media, the most common deception techniques employed are *Deception by Omission*, *Deception by Saturation* and *Deception by Spin.*

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.
- **First assumption:** the victim receiver can wholly understand and thus decode the messages it receives, which may or may not be true in the general case.
- **Second assumption:** 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.*

Shannon vs Deception by Omission

- Channel Capacity:

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

- *C* is capacity, *W* bandwidth, *P* message or signal power, and *N* noise power.
- The unwanted message is omitted and thus $P \rightarrow 0$ for unwanted information, reducing its contribution to channel capacity to zero.
- Problem? How do we map messages into *P* and *N*?

Shannon vs Deception by Omission

- Entropy Theorem – information in message:

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

- *I(m)* is information content, *p(m)* is probability of message arising.
- If $p(m) \rightarrow 1$, inevitably $I(m) \rightarrow 0$, that is messages which are certain to arise tell the receiver nothing.
- On this basis messages which are highly probable amount to noise cluttering the channel.

Defending Against Deception by Omission

- 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.
- A competent attacker will ensure that minimal opportunities exist for other channels to disclose what is being omitted.

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 may not have the available time to sort through all of the received messages.

Deception by Saturation as Active Degradation

- 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.
- Information theory provides a similar model.

Shannon vs Deception by Saturation

- Entropy Theorem – information in message:

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

- *I(m)* is information content, p(m) is probability of message arising.
- If $p(m) \rightarrow 1$, inevitably $I(m) \rightarrow 0$, that is messages which are certain to arise tell the receiver nothing.
- On this basis messages which are highly probable amount to noise cluttering the channel.
- Saturation attack - *N* and thus $N >> P$ resulting in $C \rightarrow 0$.

Deception by Saturation as Denial by Destruction

- Alternate form of *Saturation* attack is one in which the victim does have the capability to distinguish the real message from the redundant or information free messages.
- Victim is unable to perform this operation in reasonable time and thus fails to distinguish between the attacker's message and the real message.
- Shannon's model for channel capacity - the bandwidth of the channel is inadequate to the problem, that is $W << W_{required}$.

Defending Against Saturation Attacks

- If a victim expects to be subjected to a *Saturation 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.
- Saturation attacks often successful as victims are caught by surprise and cannot allocate resources to defeat the attack.

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.
- *Indirect Spin Attacks* attempt to conceal the connection between the unwanted fact and the *Subversion Attack*.

Spin Attack – Trivial Example

- 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 ….*".
- 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.

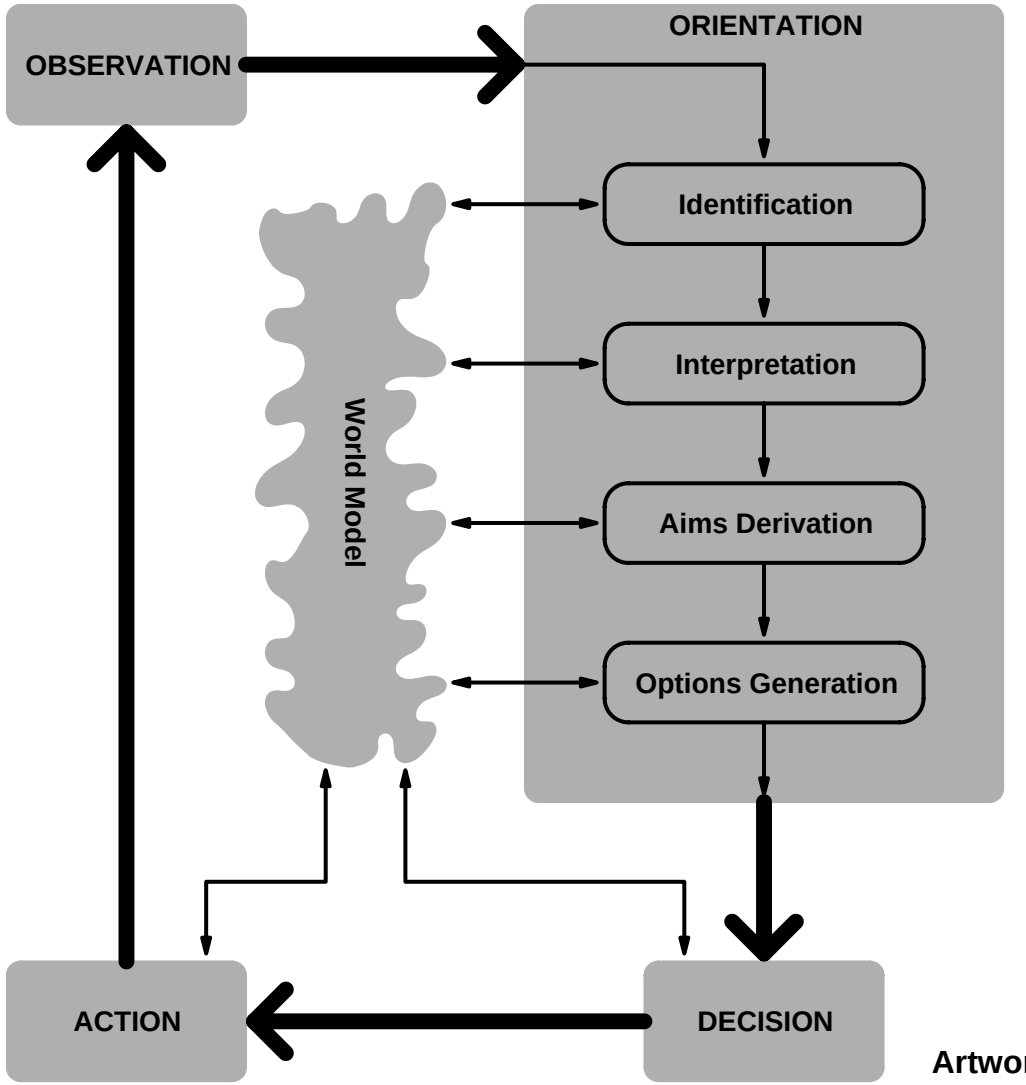
Deception By Spin

- 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.
- Spin Attacks are popular since if well executed, the attacker need not make obviously false statements to achieve the deceptive aim.

Information Theory / Processing

- *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*** (Boyd) 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).

Observation Orientation Decision Action



Artwork © 2006, L Brumley

OODA Loop Model with Expanded Orientation Step

Defending Against Spin Attacks

- 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.
- *Indirect Spin Attacks* can be very difficult to defend against.

Effectiveness

- 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.

Conclusions

1. Political and commercial marketing deceptions analysed and modelled in the framework of the four canonical strategies of *Information Warfare* and Shannon's *capacity* and *entropy* theorems.
2. Most common deceptions are *Deception by Omission, Deception by Saturation* and *Deception by Spin*, usually employed as part of compound strategies.
3. *Deception by Omission* is a form of passive *Degradation* attack.

Conclusions …

4. *Deception by Saturation* arises in two forms, the first as an *Active Degradation* attack, the second as a *soft kill Denial by Destruction* attack.
5. *Deception by Spin* is a form of *Subversion* attack, aimed at the *Interpretation phase* of the *Orientation* step of Boyd's OODA loop.
6. Defensive techniques require preparation and investment of resources or time on the part of a potential victim of such an attack.

Conclusions … Future Research

7. Relate these techniques to component phases of the Orientation step in Boyd's OODA loop.
8. Refinement of defensive strategies.
9. 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.
10. Further exploration of the relationship between message content and Shannon information to produce quantitative models.