The use of deception in systems

W. Hutchinson[1] and M. Warren[2]

[1]Management Information Systems Edith Cowan University Churchlands Geelong Western Australia 6018
Email: w.hutchinson@ecu.edu.au

[2] School of Computing and Mathematics, Deakin University, Victoria , Australia 3217
Email: mwarren@deakin.edu.au

ABSTRACT

Deception is an important element in all natural and organisational systems. This paper outlines the fundamental principles of deception, and applies them to general information systems. It examines the two fundamental methods of deception: data and context manipulation. It also briefly examines the motives for deception.

KEYWORDS: *deception, illusion, information warfare, computer security, system thinking.*

INTRODUCTION

The uses of deception in natural systems and organisations are manifest. The natural world contains innumerable examples of camouflage and behaviours whose purpose is to confuse or to create illusion. Examples include the octopus that changes colour to match the ocean bottom, or the bird that feigns injury to distract a predator away from its young. In organisations, there is a myriad of behaviours that are intended to create an illusion from ubiquitous advertising to the well-formatted and favourable annual report. In fact, deception is a fundamental aspect of strategy. Howard (1990) basically divides strategic plays into two types: those for the powerful and those for the weak. Although, it is an over-generalisation, the strong can use 'force' as their strategy, whilst the weak must rely mostly on deception to gain an advantage. Of course, the strong can use deception as well, but there are fewer requirements for them to do so.

In this paper, the word 'deception' is used to denote **an action, which changes data, objects, or context for benefit of the agency changing them**. Although the word itself tends to have a negative connotation, deception is neither 'good' nor 'bad'. Perhaps, the ethical implications of deception can be found in the motives for its use.

	Message untouched	Message manipulated
Message accepted	X	**Deceit has occurred**
Message rejected	**Deceit has occurred**	X

Table 1: Message acceptance and deception[1]

Table 1 summarises the act of deception. If a message is manipulated and the receiver accepts the message, then deception has occurred. Also, if the message has not been modified, and the receiver rejects it because of the active manipulation of the context in which the message has been interpreted, then deception has again occurred.

DATA, INFORMATION, AND KNOWLEDGE

Deception is basically about changing information, and it is to the definitions of data, information, and knowledge that this section refers. Whilst there are many meanings given to these words, in this paper's context, the most useful model is that used by Boisot (1998). In it, data is associated with a *thing*, and discriminates between different states of the thing it describes. However, knowledge is an attribute of an *agent.* Knowledge is a set of perceptions about data activated by an event. Information is this set of data filtered by the agent. It establishes a link between the agent and the data. This model is summarised in figure 1. Hence, if someone wishes to influence or attack an entity via the information derived by it, then **data** can be deleted, changed, or added; similarly the **context** that data is examined can be influenced (so influencing the interpretation of that data) - see figure 2.

[1] This table is based on an idea by Wickens (1992) in the area of Signal Detection Theory

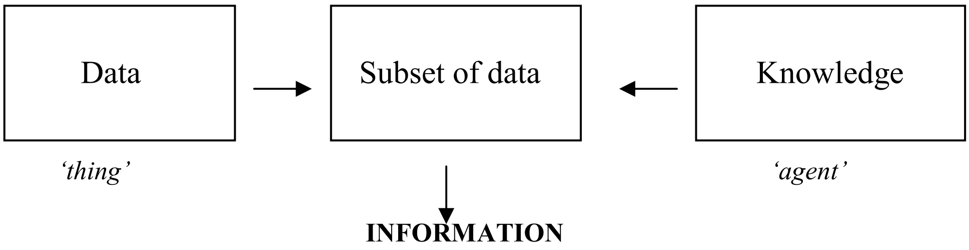

Figure 1: Boisot's Model of Data, Information, and Knowledge

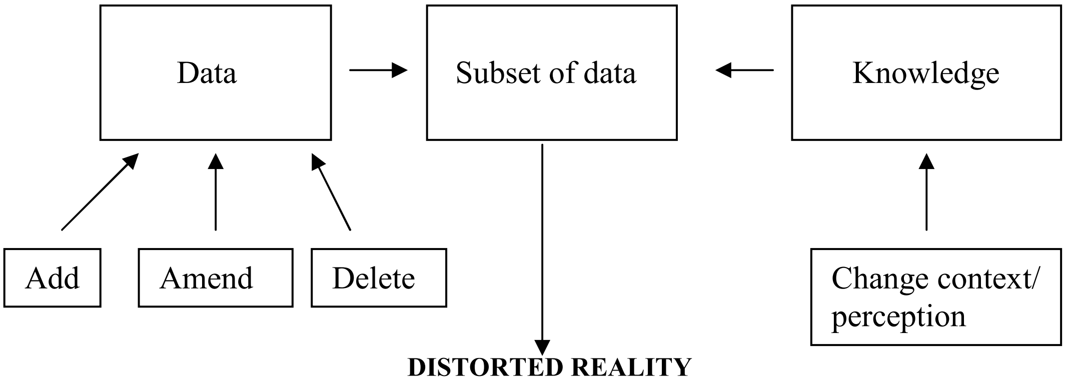

Figure 2: Tactics to produce deception

Heuer (1999, p.3) further states:

> *"People construct their own version of 'reality' on the basis of information provided by the senses, but this sensory input is mediated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural value, role requirements, and organization norms, as well as the specifics of the information received."*

Hence, people view the world through a constructed reality. Thus, deception is achieved by altering the mental models of the target, and/or the data fed to the mental processes.

TYPES OF DECEPTION

Bowyer (1982) classifies deception into two main types:

- Level 1: Hiding the real;
- Level 2: Showing the false (although this always involves 'Hiding' as well).

These fundamental types are further divided into six categories of deception:

Hiding

- **Masking**: blending in, e.g. camouflage**.**
- **Repackaging**: something is given a new 'wrapping'.
- **Dazzling**: confounding the target, e.g. codes.

Showing

- **Mimicking**: a replica, which has one of more characteristics of reality.
- **Inventing**: creating a new reality.
- **Decoying**: misdirecting the attacker.

Table 2 gives some examples of different types of deception in the natural and human worlds, whilst table 3 gives some examples found in computer/network systems.

TYPE OF DECEPTION	EXAMPLES
Masking	Camouflage found in some animals which belnds them with natural surroundings, eg stonefish, clour changes in some squids
Repackaging	Cosmetics/make-up, padded clothing, etc
Dazzling.	Ink squirted from an octopus to confuse predators, chaff discarded by Second World War bombers to confused radar
Mimicking	Bird feigning injury to distract predator from young
Inventing	Propaganda, public relations, advertising.
Decoying	Replica tanks used in Kosova war by Serbs.

Table 2: Examples of types of deception

TYPE OF DECEPTION	EXAMPLES
Masking	Stenography (Denning, 1999): hiding a message in other data.
Repackaging	Computer virus hiding in an existing program such as Trojan Horses.
Dazzling.	Encryption, codes. Sending false messages to make believe something a being carried out when it is not.
Mimicking	Web page designed to look like target's.
Inventing	Virtual reality.
Decoying	Sending information so target directs effort to an activity beneficial to the attacker, e.g. by sending false market opportunities.

Table 3: Examples of types of deception in computer/network systems

Deception is prevalent in all systems. The remaining part of this paper will be primarily concerned with deception in information systems.

USING SYSTEM FUNCTIONS IN AN INFORMATION SYSTEM AS A FRAMEWORK FOR DECEPTION

Denning (1999) listed the potential elements in an information system, which are prone to attack, they are:

- containers, eg computer and human memories;
- transporters, eg humans, telecommunication systems;
- sensors, eg scanners, cameras, microphones, human senses;
- recorders, eg disk writers, printers, human processes;
- processors, eg microprocessors, humans, software.

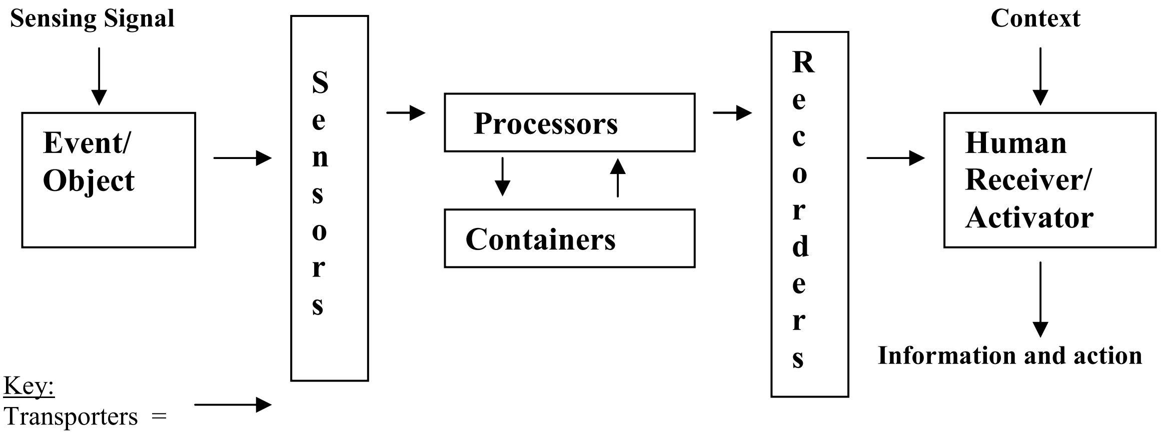

Figure 3: Components of an Information System

Each of these elements, or groupings of them, can be the focus of an attack. Thus, the range of targets can vary from public opinion to a microwave link. Figure 3 symbolises a generic information system's structure. Using this framework, tactics used to deceive can be derived.

The next section outlines each element in figure 3, and how each can effect or be affected by deception.

Sensing signal

Sensors may be active or passive. For instance, a sonar system sends out a signal. The reply is then 'sensed'. However, many sensors are passive and receive signals from an object or event without initiating a sensing signal.

In the case of active sensors, the object of deception is to disrupt this signal. For instance, the 'Stealth Bomber' scatters radar signals, which would normally illuminate an aircraft. Another ploy is to create false signals, which nullify the sensing signals. The advent of perceptual intelligence software and hardware (Pentland, 2000) which both outputs signals at the perceptual level (using tactile, visual, auditory and other types of data) and has perceptive input sensors (sensing for example, chemical, light, sound, infra-red and other environmental sensors) makes this level of deception a likely candidate for future advancement.

Object/event

This is the item to be sensed. This could range from a building under satellite surveillance to a keystroke on a keyboard. Objects can be camouflaged, and events distorted. So the building under surveillance can be made to look like a housing estate when it is really a factory, or the keystroke represents an 'A' when really the 'B' key has been pressed. The needs here are to assess 'what' is sensed, and 'how' it is recognised. It is a case of showing the sensor what you want it to see, not what is actually there or what has actually happened.

Transporters

These are the conduits through which messages flow. To deceive, the objective is to create noise around the message thus corrupting it. In electronic systems, this could mean altering the frequency, or adding/deleting transmitted data. In normal conversation, this disruption can be caused by interference such as extraneous noise, blinding light, or uncomfortable environmental conditions.

Sensors

Here the objective is to either 'blind' the sensor to incoming signals (for example, an electromagnetic pulse with electronic equipment), or to feed the sensor signal that you want it to sense. For example, if submarines can be tracked by satellite monitors from the bioluminescence created by their propellers, then creating similar bioluminescence where there are no submarines will 'fool' the sensor.

A number of bogus Web sites do this. The idea of 'spoofing' uses this principle.

Processors

Here the main objective is to alter the logic of the process to achieve the output desired. In computer systems this can be achieved by alteration of program logic (for example by a 'virus'), or parameters fed to those programs.

Containers

These data stores can help deception if the data is amended, deleted, or added to in a beneficial way to the attacker. Hacking into databases to change their contents is an example of this.

Recorders

Very much like the sensors, the objective is to corrupt the output (rather than input) stream formation. Manipulating the workings of these mechanisms (or their logic if separate from main process logic), in a meaningful way to the attacker, can provide benefits.

Context

All data is interpreted in a certain context. The objective of the deceiver in this element of the chain is to manage perception. Military style Psychological Operations, or commercial style advertising/public relations can achieve this. The aim is to produce an environment in which the human will interpret the data in a specific way.

Human Receiver/Activator

The data produced by the system, and the context it is perceived to be in, results in Information Creation and Action. In a completely automated Artificial Intelligence system, corruption of the rules, upon which decisions are made, could cause deception to occur (also perceptual intelligence systems, mentioned previously can fall victim to this). In human subjects, direct mind manipulation can also achieve this. Such things as behaviour modification (for example, reinforcement, conditioning, punishment), hypnotism, brain washing, or psycho-drugs can cause a deceptive process to occur.

The brief summary above shows the wide range of option when planning a deception. The following section will examine what the motivations are for deceiving individuals and organisations.

MOTIVES FOR DECEIVING

As deception is a conscious activity, it can be assumed that it requires some form of motive. Ford (1996) gives some insight into the types of lies and their associated motives for individuals. This classification of lies can also be profitably used with organisations. Table 4 summaries Ford's findings with the authors' additions for organisational motives.

Type of lie	Individual's motive	Organisational attacker's motive
Benign and salutary lies	To effect social conventions	To effect or destroy a good corporate public image
Hysterical lies	To attract attention	To attract attention for example
Defensive lies	To extricate oneself from a difficult situation	To extricate (or involve!) the organisation form a difficult legal/corporate image situation
Compensatory lies	To impress other people	To impress clients, the public, etc.
Malicious lies	To deceive for personal gain	To obtain market share, fraud
Gossip	To exaggerate rumours maliciously	To compromise a competitor
Implies lies	To mislead by partial truths	Disinformation to protect/harm the organisation
"Love intoxication" lies	To exaggerate idealistically	To promote/discredit the organisation
Pathological lies	To lie self destructively	Unusual, possibly to lower the value of a company for buy-out, etc.

Table 4: Types of lies and motivations for using them

It can be seen that deception can be used both to protect the organisation/individual, and to compromise a competitor. Deception is pervasive. Its effects can be regarded as both beneficial (for example, increased sales) or costly (for example, buying a product not required).

THE FUTURE

The coming of the Information Age has provided new avenues for deception. The world of virtual reality, the storage of vast amounts of vulnerable data in digital format, and the increasing availability of information technology has created a need for more research into such areas as data integrity, computer forensics, and the use of networks for propaganda. All of these require an understanding of the principles of deception, if for no other reason than to counter it.

The increasing use and sophistication of surveillance technology may also spur the use of deception to maintain privacy, or an illusion of a required personal or corporate image. The following decades might see the Information Age replaced by the Age of Deception.

REFERENCES

Boisot, M.H. (1998) *Knowledge Assets*. Oxford University Press, Oxford.

Bowyer, J.B. (1982). *Cheating*, St.Martin's Press, New York.

Denning, D.E. (1999). *Information Warfare and Security*, Addison Wesley, Reading: Mass.

Ford, C.V. (1996) *Lies! Lies!! Lies!!! The Psychology of Deceit*, American Psychiatric Press, Washington.

Howard, M. (1990) *Strategic Deception in the Second World War*, W.W. Norton & Co Ltd., London

Heuer, R.J. (1999) *Psychology of Intelligence Analysis*, Centre for the Study of Intelligence, Central Intelligence Agency, USA.

Pentland, A (2000) Perceptual Intelligence, *Communications of the ACM*, **43**, 3. 35-44.

Wickens, C.D. (1992) *Engineering Technology and Human Performance*. Addison-Wesley.