Information Warfare and Deception

William Hutchinson
Edith Cowan University, Perth. Australia

w.hutchinson@ecu.edu.au

Abstract

This paper examines the history of the phenomenon of Information Warfare and the increasingly dominant role that deception is taking within its framework. The concept of information warfare began as a technology oriented tactic to gain information dominance by superior command and control. This soon developed into a realization of the power of information as both a 'weapon' as well as a 'target'. The importance of information rather than its associated vehicle – information technology − created a situation where influence became a critical factor in conflict. As the nature of conflict changed to being an almost ongoing situation, control over mass communication became a high priority task for governments as well as the military. As such, the manipulation of information became an essential function. Thus, the world of deception became an integral part of official communications between governments and their constituency.

Keywords: Deception, Information Operations, Information Warfare.

Background

This paper examines the development of the concept of information warfare in Western liberal democratic countries – predominantly the United States. In addition, the chapter illustrates importance and increasing dominance of deception within the framework of Western information warfare practice.

The origins of the term 'information warfare' can be traced back to the late 1980's when the expression was specific to the military domain. It became a 'living' concept in the Gulf War of 1991. Information warfare's origins are electronic warfare, military deception, psychological operations and information/operational security. However, the most significant element in its evolution was the development of electronic computing and communications technology. By the 1990's, the role of this technology in warfare had been proven in the 1991 Gulf War (Campen, 1992). Information or more specifically, information technology had given the edge in battlefield intelligence, targeting, and command and control. However, the emphasis was still on the technology rather than the 'information' *per se*. Nevertheless, another component was developing in this war – media management. Since the war in Vietnam, the military had been developing their tactics. The war in Vietnam was a watershed for the relationship between the media and the military (and thus, government). Reporting from the Vietnam War was, largely, an open situation for journalists (Louw, 2005). However, even in this conflict, official press briefings tightly controlled information flow. Nevertheless, the development of helicopter transport and a cooperative military gave reporters opportunities to go out on operations in an uncontrolled *ad hoc* way. The images sent back to be broadcast to the televisions in the homes of America were quite powerful. The military partially blamed the subsequent debacle on this freedom of movement by journalists. In addition, the military blamed the iconic images that emerged for the loss of the 'home front' and, subsequently, the war (Carruthers, 2000). The military and the government did not realise the potential of television and its potential to influence public opinion. Subsequent media and propaganda tactics used by the Western powers were to alter significantly from this point. In America, the development of these tactics was to threaten even the viability of the First Amendment of the Constitution (Carpenter, 1995).

The Falklands War in 1982 set the scene for the dissemination of official information releases in other conflicts in that decade such as the invasions of Grenada and Panama. The Falklands War was fought in a geographically isolated area with very limited communications available for anybody except the military. As such, all press releases were controlled and communicated by the government. Journalists with the task force were vetted and all their reports went through military censorship (Street, 2001). It was a classic case of manipulating the data presented to a population. The United States learned from this experience and severely constrained reporters during the invasion of Panama (Cook & Cohen, n.d.). Added to this was the manipulation of the context in which it was interpreted. Victory parades were staged showing 'Panamanians' celebrating the American involvement. The image transmitted back to America was that of a jubilant Panamanian population when, in reality, the invasion was looked upon with resentment in the indigenous population. However, the perception that the military operation was not only a success, but welcomed by all parties, was all that mattered. The country had been liberated from oppression – that was the message.

The Gulf War in 1991 showed a level of sophistication in information control by the military and government that was to influence the way that Western governments were to handle public perceptions for the next decade. The creation of press 'pools' and 'approved' journalists basically meant that journalists would only report the data given to them by government or military officials. Independent journalists were kept away and, in fact, were treated as potential enemies. A compliant media ensured that only the government's version of events would be presented (Knightley, 2000; Taylor, 1992).

By the mid-1990's information warfare, driven by considerable developments in computer and communications technology, was developing into an integrated doctrine. It was still technology focused with command and control dominating, and with media management still as a separate entity. However, technological innovations were beginning to see them merge. It was becoming clear that modern wars were also media wars. However, information warfare was still predominantly military in nature and it was assumed to only be relevant to a wartime context. During this time an influential text was written that outlined the scope of information warfare (Libicki, 1995). The text suggested that information warfare was a combination of command and control warfare, intelligence based warfare, economic warfare, cyber-warfare, and hacker warfare. These terms were loosely defined but really stated that information warfare was about using technology to assist in command and control and intelligence gathering whilst, at the same time, trying to disrupt your enemy's equivalent processes. The inclusion of economic warfare is an anomaly although, at the time, there was much discussion on this threat to America's security (Fialka, 1997).

At the same time in the separate areas of public diplomacy and public affairs, were going through fundamental changes. Western governments were changing their relationships with their publics. Whilst, misrepresentation of facts had occurred throughout history, a new breed of public relations professionals were taking the works of Bernays (1928) and Lippmann (1922) from the 1920's and the capabilities of modern communications, to aggressively use information as an asset. Information was no longer an element to be created but to be disseminated in a controlled fashion and, if necessary, to be created at will. The art of selecting appropriate information beneficial to the instigator which led to misinformation (*misleading* information) had been cynically replaced by the use of disinformation – the *deliberate* use of misleading information. This subtle change from 'spin' to deliberate lying was changing the nature of the government-military-media-public interface.

This subtle change in relationship went unnoticed at first. Deception was not thought to be an important factor in public-government contact in the West. This was thought to be more a characteristic of totalitarian regimes. For instance, in the Marxist-Leninist Soviet Union there was little distinction between the military and diplomatic facets of government. Deception was a function of state craft and not confined to the military (where it was an accepted practice in wartime, even with Western publics). The doctrine of deception became known as *maskirovka* (loosely this word means 'deception', although translators also use the words 'concealment' and 'camouflage' to express the English meaning (Smith, 1988, p.1). Broadly, the Soviet concept of *maskirovka* includes deception, disinformation, secrecy, feints, diversions, imitation, concealment, simulation and security (Shea, 2002, p.2) although it is not restricted just to these. Basically, it is concerned with "anything capable of confusing, and therefore weakening, the enemy" (Lloyd, 1997, p. 115).

In Marxist-Leninist thought, war is an extension of politics and deception pervades it. Initially, the Soviets thought that deception was especially needed in the period just before the outbreak of hostilities (Glantz, 1987, p.179) but later this thinking developed into the idea that *maskirovka* should be practiced continually. In the Soviet's mindset, anti-Marxist nations use all tools – economic, political, military, and diplomatic – to destroy a socialist system. Hence, all of these were part of the war effort; therefore, deception could, and should be, used in all these elements of statecraft both in times of 'peace' and war. This was a function of Marxist thought rather than military in nature. The logic was that as socialist states were always at war against the capitalists (who were incessantly trying to destroy them), then war was also constant whether overtly stated or not. Hence, deception can be justified at any time as socialism was 'good' and 'moral' and anything that wanted to destroy it was 'bad'; thus whatever was done to support socialism was good – the end justifies the means. The Soviets did not hold the concept of deception in the same moral disdain as it was in the West. However, at the turn of the twenty first century, Western governments were seeing the potential of deception as a tactic, if not a strategy. When this change in mindset did occur, the role of the manipulation of information for advantage came to the forefront. It was the access to and the use of information that were the fundamental determinants of superiority. The practice of deception is a natural extension of the acceptance of information as the dominant element in competitive advantage. If information is of value in decision-making, then its control and manipulation must also be important.

During the 1990's, the development of an oligopoly of global, media companies with strong ties to the established governments such as, CNN, Disney and Sony (Street, 2001), were starting to create a mass media that was compliant and susceptible the government perspectives, and prepared to purvey whatever 'information' it was fed by official sources. At the same time, 'information warfare' was relegated and another term coined – 'information operations'. 'Information warfare' was now that subset of information operation specific to wartime situations. There was an acceptance in Western countries that manipulation of information was an acceptable, if not essential, practice. Hence, the practices of information warfare were legitimate in peacetime as well.

The twenty first century saw the evolution of 'media wars' into a truly integrated process. Governments and their associated militaries had matured their techniques for influencing the public. The public relations techniques developed in the 1920's had been refined with the exponential growth in knowledge. Social psychology theory and empirical research were merging with psychological warfare and public diplomacy techniques. This combination assisted by sophisticated media technologies and techniques, as well as monopolistic media companies were to develop into a situation where the media was to be an intrinsic part of the war effort.

The terrorist attacks on New York, Washington and Pennsylvania (9/11) severely affected the ‘objectivity’ of reporting. Journalists now saw themselves as part of the national ‘team’ rather than ‘outsiders’ who relayed information impartially. The consequences of this attitudinal shift in reporters’ perceptions of their role were to become clear in the subsequent years. The second war with Iraq in 2003 was to show the reality of a true ‘information war’ and the importance of the media.

In a sense, the second Iraq war was a continuation of the first. However, the fighting environment of these wars was different. Whilst there were commonalities such as the combatants and the desire of the military and government to severely restrict and control reporting, the global and social contexts were radically different. Nevertheless, media and military relations and behaviours had a common thread, albeit that different tactics were use. In both wars, the dominance of the military perspective pervaded the reporting effort. The control of broadcasted images during the ‘official’ war was almost total. In a world of ubiquitous communications, this was an incredible outcome for the military communication’s effort. A single message tended to dominate the coverage by the monolithic Western media – few dissenting voices were heard or controversial images shown. The ‘inter-war’ years when the conflict was not ‘official’ the coverage was different for each period although the effect was the same.

The comment by Baurillard (1995) that the first Gulf War ‘did not take place’ is also relevant for the second Iraq war in 2003. Baurillard did not mean that the war had not physically taken place but that the war the public knew of was an illusion created by the war machine. The media coverage for both wars became *militainment* where the military-entertainment sports complex (Schwartz, 2004) gave blanket coverage with its own suspense, drama, and excitement. The war in 1991 mostly showed smart weapons with cameras attached flying through windows in ‘surgical’ strikes. However, in both wars, use was made of what Kate Adie (2004) calls the ‘sexiness’ of weapons; the visual spectacular of explosions on the horizon after the rocket or cruise missile is launched gives immense gratification. However, what the media rarely showed were the destructive consequences of those explosions such as dead or mutilated bodies, or ruined buildings.

The *medium was now the message* (to paraphrase McLuhan, 1964); or as General Franks said in 2004, the media was now the ‘fourth front’ (a play on the term ‘The Fourth Estate’). Truth could be and was manipulated by a compliant mass media where they communicated the majority of information about the world outside the individual (see Miller, 2004). Mass perceptions of events were controlled by various means. Inyengar and Simon (1994) posit that there are three classes of media effects:

- Agenda setting – the ability of the media to define the significant issues of the day.
- Priming – the relationship between patterns of news coverage and the criteria with which the public evaluated politicians.
- Framing – the connection between qualitative features of the news and public opinion.

These authors claim that dramatic changes in public opinion are determined by the amount of news coverage about certain political issues. This coverage will dictate the level of importance the public gives to these issues – this is ‘agenda setting’. The media also has the ability to affect the way politicians are perceived – this is ‘framing’. This is really an extension of ‘agenda setting’ and describes the impact of the weightings assigned to specific news issues. Priming tends to be stronger for performance evaluation and have lesser effects for personality assessments. Thus, agendas, perceptions and relationships between events could be controlled. People can only perceive from the data that they receive (Boisot, 1998).

Information and its communication were now completely controlled at the mass level. The influence of information warfare (especially the psychological operations and deception components) was paramount. In a sense, perception became more important than reality. Even the impact of the Internet and the 'free' exchange of information made no mass impact on social perceptions. In fact, the advent of 'blogging' (the use of Web logs to transmit messages or diaries access the Internet) by individuals 'reporting' events as they 'saw' them in the 2003 Iraq war eventuated in the development of deceptive blogging by the authorities to confuse and counteract. Deception had taken on a global, postmodern dimension – nothing was real.

Information Warfare and Deception in Military Doctrine

Information warfare is primarily a construct of a 'war mindset'. However, the development of information operations from it has meant that the concepts have been transferred from military to civilian affairs. The contemporary involvement between the media, the military, and the media in the contemporary world of the 'War on Terrorism' has meant the distinction between war and peace is difficult to make. However, below the application of deception in the military context is described but it must be added that the dividing line is blurred.

Of course, deception has been an attribute of humans throughout history. Its informal use in war also has a history as long as war itself. However, only in the twentieth century with its formal use by governments and the military did the development of its theoretical base begin. The Soviet Union used *Maskirovka* to great effect during the Cold War and was first to develop it as an integrated part of normal diplomatic and military procedure (Smith, 1998). It also became a formal part of doctrine in Western militaries in that late twentieth century.

The U.S. Joint Doctrine for Information Operations (Joint Pub 3-13, 1998) defines deception as:

> *Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in manner prejudicial to his interests*

However, the Joint Doctrine for Military Deception (Joint Pub 3-58, 1996) gives a fuller definition:

> *Military deception is defined as being those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission.*

A later doctrine from the US Air Force (2005) on information warfare (actually, information operations) refers to 'influence operations' as one of the four major components of the information environment (network warfare operations, electronic warfare operations and integrated control enablers are the others). The components of *influence* operations are psychological operations, military deception, operations security, counter-intelligence, public affairs, and counter-propaganda. All of these activities have one aim: to influence the mind and behaviour of the adversary in ways beneficial to the perpetrator. As such, all involve deception to a greater or lesser degree. This is in contrast to a decade earlier where the emphasis was on technology and its use. The objective of deception is to be used with the other tactics to gain 'information superiority' where this is defined as "the state that is achieved when a competitive advantage is derived from the ability to exploit a superior information position" (Alberts, Gartska, & Stein, 1999, p.32). It is attempting to get the adversary to believe what the deceiver wants them to believe for the advantage of the deceiver and the disadvantage of the deceived. It is truly using information as a weapon. Information superiority is the *raison d'être* of information warfare

The theory of deception was also developed outside the formal doctrinal area. For instance, since the mid-1990's investigators from RAND examined the use of deception and its theoretical basis and produced a model for deception planning (see Figure 1).

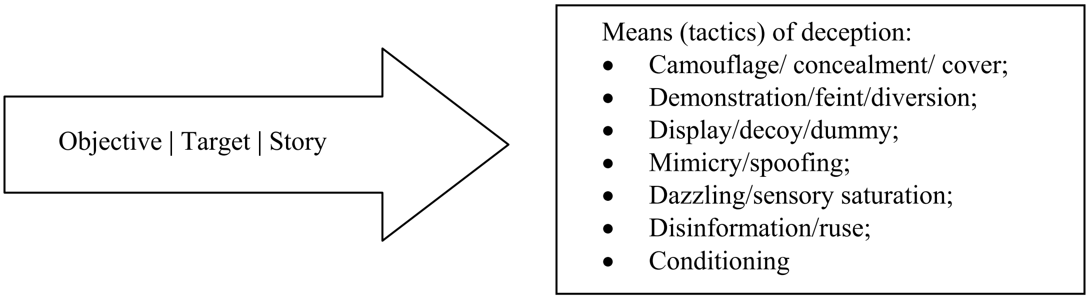
Objective | Target | Story
Means (tactics) of deception:
• Camouflage/ concealment/ cover;
• Demonstration/feint/diversion;
• Display/decoy/dummy;
• Mimicry/spoofing;
• Dazzling/sensory saturation;
• Disinformation/ruse;
• Conditioning

Figure 1: The Deception Planning Process (after Gerwehr & Glenn, 2000, p.26).

This model couples the techniques available with the intuitive notion that for a successful deception there must be an objective (to measure your success by), a target audience (to choose the applicable means of deception), a story (as a vehicle for the deception), and a means.

Further ideas came from Hall (2003). Here the target and one's knowledge of it, as well as the target's view of the 'attacker', must be taken into account. Without adequate appreciation of the target then no deception can really be envisaged or stand a chance of being successful. The actual components that need to be considered are given in Table 1.

Table 1: Red and Blue Wargaming Construct for deception (after Hall, 2003, p.33)

Red's view of Self	Red's view of Blue	Red's view of Blue's view of self	Red's View of Blue's View of Red
Blue's view of self	Blue's view of Red	Blue's view of Red's view of self	Blue's view of Red's view of Blue.

However, these models are really no more than the formalization of the knowledge already known. Nevertheless, although simplistic, they provide a framework for rationally designing deception campaigns.

Much of the RAND work was derived from work completed in the 1980's. For example, in 1986, a volume was published (Mitchell & Thompson, 1986) that attempted to theorize about deception in the natural and human worlds. This text appears to have had some influence on others developing a theoretical approach to deception. In it, Mitchell states that deception occurs when the following is true:

> *(i) An organism R registers (or believes) something Y from some organism S, where S can be described as benefiting when (or desiring that)*
>
> *(iia) R acts appropriately toward Y, because*
>
> *(iib) Y means X; and*
>
> *(iii) it is untrue that X is the case.*

In the same volume, Russow (1986) attempts to explain the cognitive state of a deceiver by stating that:

> *An organism S can be said to deceive D if and only if S's effect on D is a causal factor in D's having a false belief that it is in situation A, where D's acting on that belief is more advantageous to S than D's acting on the belief that it is situation B (the actual situation).*

Also

> *An agent's behaviour is deceptive if and only if the agent intends that, because of its behaviour, another organism will come to (and perhaps act on) a false belief.*

These definitions are applicable to both the animal and human worlds. Whilst the volume is mostly dedicated to animal deception, it also includes papers on deceptive design (Thompson 1986), cultural typologies of deception (Anderson, 1986) and military deception (Sexton, 1986) which have been influential in the development of state and military deception practices.

In 1991, J Bowyer Bell and Barton Whaley published *Cheating and Deception* as an attempt to theorize about the nature of deception in its broadest sense. They created a classification of deception types. In it, they speculated that there were two basic types of deception:

- Level 1: that consisted of ***hiding the real***, and
- Level 2: this ***showed the false***.

Of course, Level 2 is always a part of level 1.

These fundamental types are further divided into six categories. **Hiding** can be broken into: ***masking*** (basically means blending in for example, camouflage), ***repackaging*** (where something is given a new 'wrapping'), and ***dazzling*** (which consists of confounding the target for example, using codes). **Showing** can be broken into: ***mimicking*** (this means producing replicas, which have one or more characteristics of reality), ***inventing*** (which involves creating new realities), and ***decoying*** (which involves misdirecting the attacker).

These theoretical constructs gave researchers a framework for the development of frameworks such as the RAND example in Figure 1. However, it must be admitted that relatively little has progressed passed these models based on natural deceptive phenomena.

Deception and Information Warfare Tactics

Information warfare is split into offensive and defensive modes. Deception has its place in the offensive mode although counter-deception (which is defined as "efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation - Joint Pub 3-13, 1998, p. GL-5) is regarded in U.S doctrine as defensive. However, the distinction is somewhat artificial and, as will be illustrated below, it can be used in all the elements of information warfare.

Information warfare (information operations) consists of various functions (from Joint Pub, 3-13, 1998). These include defensive activities such as: operations security (this denies knowledge of your own operations to the enemy), counter deception (decreases the effect of an enemy's deception activities), and counter propaganda or counter psychological operations (which attempts to counter the impact of the enemy's messages). Offensive activities include: military deception (measures designed to mislead the enemy by manipulation, distortion and falsification of evidence), and psychological operations (measures to influence attitudes and behaviour of allies and enemies).

Added to these are the closely aligned Public Affairs (see Joint Pub, 3-61, 1997) and Civil Affairs (Joint Pub 3-57.1, 2003). Public Affairs is concerned with military/government interaction with the media, whilst Civil Affairs is concerned with those actions needed to influence the relations between the military and the civilian population in a military operation. American sources are used in this paper as they are the most published. For instance, the Australian and Untied Kingdom doctrines for information operations have a classification of 'Restricted'.

The Significance of Deception in Contemporary Information Warfare

Information warfare in the Information Age is about controlling the 'infosphere'. It includes perceptions and information flows at the tactical, operational and strategic level in times of peace, tension, and war. As such, it means controlling sources and the dissemination of information. Controlling perceptions held by those in the infosphere implies that information must be created that favours the dominant party. As such, that information may or may not represent physical reality. In other words, "information that favours the dominant party" might be a subset of 'reality' or, in fact, an 'artificial reality'. Either way, if it represents a favourable subset of reality or a favourable 'illusory reality' then it constitutes deception.

By definition, information warfare is about using and protecting information. This begs the question: what is 'information'? The conventional way to define the words 'data', 'information' and 'knowledge' is in a linear fashion. Using this approach, 'data' describes attributes of things; 'information' is collated data in context; and 'knowledge' is information that an individual has interpreted in the light of experience. In the information warfare context, Boisot's (1998) model provides a more useful definition. In his model, 'data' is associated with a *thing*, and discriminates between different states of the thing it describes. It consists of attributes of the events or objects it describes. On the other hand, 'knowledge' is an attribute of a *human*. Knowledge is a set of interacting mindsets about data activated by an event. Information is the set of data filtered by the human within the bounds of the knowledge held by that human (or group of humans); it establishes a link between cognition and data.

Thus, the ***defensive*** side of information warfare is concerned with the protection and integrity of data, people within the systems and the technological enablers that allow the creation and communication of information. It makes sure that data is available in a timely manner, has high integrity, and is only available to those people or systems that have authority to use it. Figure 2 uses Biosot's model as the basis to show the ways in which each of the elements can be attacked.

A contemporary phrase is that of 'denial and deception' (further explained in Godson & Wirtz, 2002). The function of 'denial' is to secure the information and assist deception, whilst that of 'deception' itself is to use the attack methods in figure 2 to gain advantage over an adversary.

Thus, defensive information warfare's main function is to prevent these attack methods from being successful, whilst offensive information warfare's uses the same methods against a foe. According to the model in Figure 2, the major methods of deception are:

- Presenting data to the adversary that represents the truth as you would want them to perceive it. This is achieved by presenting a tailored subset of 'real' data, and/or manipulated data, and/or depriving the foe of any data, and/or disrupting the foe's data collection, and/or
- Setting the context in which the foe interprets that data, and/or
- Producing 'noise' in the communication channel so that the foe receives only the data allowed by the deceiver.

The methods above show the importance of the interdependencies between the other factors of information warfare. For instance, security should ensure only the data that fulfils one's objectives are released (even if they are false sometimes), and psychological operations should create the context in which it is to be interpreted. In this case, it is possible to create a deception with all 'true' data; it is just that it will only be a subset of the real, and/or will be interpreted in the incorrect way as it will be presented in a controlled context. In a sense, all offensive information warfare is deception as it is 'hiding the real' from the enemy even if it is not always 'showing the false'.

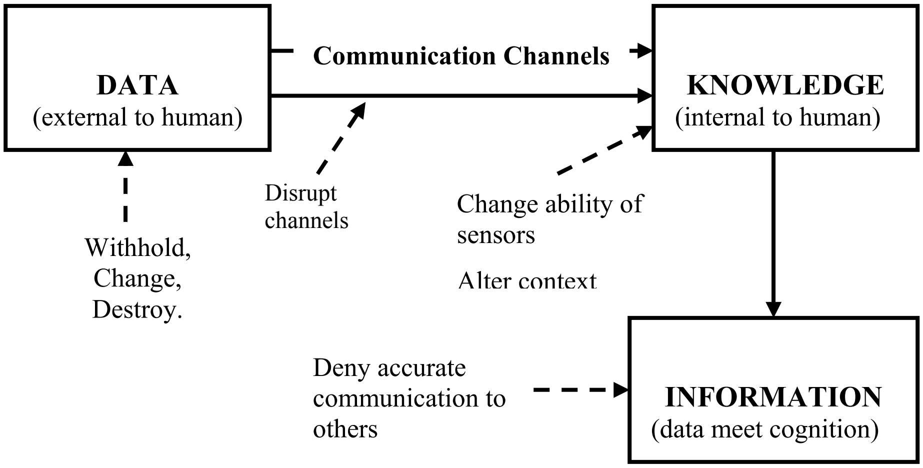

Figure 2: The relationships between data, context, knowledge, information; and the methods by which each element can be attacked to cause deception and corrupted information.

Conclusion

By definition, information warfare has information and its use as a weapon as the core of its activities. As deception is about limiting access to and manipulation of information, it is a fundamental requirement for successful information warfare. This permeates all its levels: tactical, operational and strategic.

Arquilla and Rondfelt (1996) describe nations as being at different stages in the development of a networked society. They proffer four stages: clan/tribal, institutional, market, and organizational networks. Developed nations such as America, Australia, and the United Kingdom would fit into the latter category. As much of the data storage and processing, and communications is achieved by electronic networks in these nations, digital deception would take prime place. In other less developed nations, other methods would take prominence. In developed and developing nations, the combination of mass media and communication networks has provided a rich, if challenging, environment for information warfare and deception. Ironically, this 'information rich' environment makes deception both more and less achievable. The ubiquity of communications makes the dissemination of data much easier. Hence, people have access to various views. However, the context with which this information is interpreted is primarily determined by the mass media that is generally owned by small cartel of interests. It is in this paradoxical world that future deceivers will work.

References

Adie, K.. (2004). [Television presentation]. *Press Club,* Australian Broadcasting Corporation, 13.00hr, 22 December 2004.

Alberts, D.S, Gartska, J.J., & Stein, F.P. (1999). *Network centric warfare: Developing and leveraging information superiority*. Washington: CCRP.

Anderson, M. (1986). Cultural concatenation of deceit and secrecy. In R. W. Mitchell & N. S. Thompson (Eds.), *Deception: Perspective on human and nonhuman deceit* (pp. 323-348). Albany: State University of New York Press.

Arquilla, J., & Ronfeldt, D. (1996). *The advent of netwar*. Santa Monica, CA: Rand Corporation.

Baudrillard, J. (1995). *The Gulf War did not take place*. Sydney: Power Publications.

Bell, J.B., & Whaley, B. (1991). *Cheating and deception.* New Brunswick, USA: Transaction Publishing.

Bernays, E. (1928). *Propaganda*. Brooklyn, NY: Ig Publishing.

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

Campen, A. D. (Ed.). (1992). *The first information war: The story of communications, computers, and intelligence systems in the Persian Gulf War.* Fairfax, VA: AFCEA International Press.

Carpenter, T.G. (1995). *The captive press: Foreign policy crises and the first amendment*. Washington, DC: Cato Institute.

Carruthers, S.L. (2000). *The media at war*. Houndsville: MacMillan Press.

Cook, M., & Cohen, J (n.d.). *The media goes to war: How TV sold the Panama invasion.* Retrieved 4 September, 2005, from: http://www.totse.com/en/media/the_media_industrial_complex/165624.html

Failka, J.J (1997). *War by other means: Economic espionage in America*. New York: W.W Norton.

Gerwehr, S., & Glenn, R.W. (2000). *Unweaving the web: Deception and adaptation in future urban operations*. Santa Monica, CA: RAND.

Glantz, D.M. (1987). The red mask: The nature and legacy of Soviet military deception in the second world war. In M.I.Handel (Ed.), *Strategic and operational deception* (pp: 175-259). Totowa, NJ: Frank Cass.

Godson, R, & Wirtz, J.J (2002). *Strategic denial and deception*. New Brunswick: Transaction Publishers.

Hall, W. (2003). *Stray voltage*. Annapolis: Naval Institute Press.

Iyengar, S., & Simon, A. (1994). News coverage of the gulf crisis and public opinion. In W. L. Bennett & D. I. Paletz (Eds.). *Taken by storm – The media, public opinion, and U.S. foreign policy in the Gulf War* (Ch. 8, pp.167 - 185). Chicago: University of Chicago Press.

Joint Pub 3-13 (1998). *Joint doctrine for information operations*. Joint Chiefs of Staff, 9 October, 1998.

Joint Pub 3-37.1 (2003). *Joint doctrine for civil affairs*. Joint Chiefs of Staff, 14 April, 2003.

Joint Pub 3-58 (1996). *Joint doctrine for military deception*. Joint Chiefs of Staff, 31 May, 1996.

Joint Pub 3-61 (1997). *Doctrine for joint public affairs*. Joint Chiefs of Staff. 14 May, 1997.

Knightley, P. (2000). *The first casualty*. Baltimore: John Hopkins University Press.

Libicki, M. (1995). *What is information warfare?* Washington: National Defense University.

Lippmann, W. (1922). *Public opinion*. New York: Free Press.

Lloyd, M. (1997). *The art of military deception*. London: Leo Cooper.

Louw, E. (2005). *The media and the political process*. London: SAGE Publications.

McLuhan, M. (1964). *Understanding media*. London: Routledge.

Miller, D. (Ed.). (2004). *Tell me lies: Propaganda and media distortion in the attack on Iraq*. London: Pluto Press.

Mitchell, R.W., & Thompson, N.S. (Eds.). (1986). *Deception: Perspectives on human and nonhuman deceit*. Albany: State University of New York Press.

Russow, L.M. (1986) Deception: A philosophical perspective. In R. W. Mitchell & N. S. Thompson (Eds.), *Deception: Perspective on human and nonhuman deceit* (pp. 41-52). Albany: State University of New York Press.

Schwartz, J. (2004). A cast of thousands: The media and the staging of Gulf War Two. *Australian Screen Education*, *22*, 52-57.

Sexton, D.J. (1986). The theory and psychology of military deception. In R. W. Mitchell & N. S. Thompson (Eds.), *Deception: Perspective on human and nonhuman deceit* (pp. 349-356). Albany: State University of New York Press.

Shea, T.C. (2002). Post Soviet maskirovka, cold war nostalgia, and peacetime engagement. *Military Review*, *May/June*, pp.63-67. Fort Leavenworth, Kansas: Command and General Staff College.

Smith, C.L. (1988). Soviet maskirovka, *Aerospace Power Journal, Spring*.

Street, J. (2001). *Mass media, politics and democracy*. Houndmills: Palgrave.

Taylor, P.M. (1992). *War and the media: Propaganda and persuasion in the Gulf War*. Manchester, UK: Manchester University Press.

Thompson, N.S. (1986) Deception and the concept of behavioral design. In R. W. Mitchell & N. S. Thompson (Eds.), *Deception: Perspective on human and nonhuman deceit* (pp. 53-66). Albany: State University of New York Press.

U.S. Air Force (2005). Information operations. Air Force Doctrine 2-5, 11 January, 2005.

Biography

William (Bill) Hutchinson is the IBM Chair in Information Security at Edith Cowan University, Perth, Western Australia. He is the Chief Editor of the Journal of Information Warfare (www.jinfowar.com), and Chair of the Australian Information Warfare and Security Conference. He is a member of the Australian Institute for Professional Intelligence Officers, and co-author of *Information Warfare: Corporate Attack and Defence in a Digital World*. He is author of numerous papers on Information Warfare. His research concentrates on issues in Information Operations specifically propaganda, influence, and deception.