The Impact of

ISTAR on Military Deception

'Deception is the distortion of perceived reality: it is done by changing the pattern of distinguishing characteristics of a thing (object or event) as detected by the sensory system of the target. Magicians call this magic – soldiers call it deception.' [1]

B. Whaley

Deception comprises 'measures designed to mislead the adversary that include manipulation, distortion and falsification in order to induce him to act in a manner prejudicial to his interest'.[2] In inducing an adversary so to act, surprise [3] will be attained and deception is, therefore, a natural weapon in the manoeuvrist arsenal: the adversary is induced to prepare for one Course of Action (CoA) while friendly forces will act in another manner or at a different tempo. Deception is not a substitute for military leadership or warfighting [4] but, as a force multiplier, it is often attractive when the balance of force is against the practitioner. However, it should also be considered valuable to a superior force not only on grounds of economy of effort [5] but also in the furtherance of manoeuvrist operational art as 'strength unaccompanied by strategem will become sterile and lead to a general decline'.[6] British Defence Doctrine (BDD) recognises the worth of deception as a means to shape an opponent's perceptions [7] and United Kingdom (UK) operational doctrine [8] calls for a deception plan to be considered during the estimate process. However, despite being enshrined in doctrine, many consider that there has been a lack of military deception folllowing World War 2 (WW2) and, since that era, the battlespace has also altered in a variety of ways. Does deception, therefore, remain applicable today? Alterations have included the nature of operations, the international security system and 2, primarily technological, factors that will form the focus of this essay. However, the non-technological factors will first be briefly outlined because they are germane to the overall argument.

Initially, it will be useful to query the apparent lack of deception since WW2, and explore some human factors pertinent to its employment. Since WW2, UK forces have been involved not only in small-scale operations in post-colonial countries such as India, Malaysia (Counter-insurgency (COIN) operations) and Kenya [9] but also in major Coalition operations such as the 1991 Gulf War and Bosnia-Hercegovina; and the UK conducted operational deception in support of the San Carlos landing in the Falklands Conflict.[10] The United States (US), Israel, Egypt and the Soviet Union (SU), among others, have all employed notable operational and strategic deception plans since WW2 but the extent of employment has been related to the nature of the conflict and the relative strengths of the protagonists. A common belief allied to the myth of the absence of deception is that because Former Soviet Union (FSU) and Chinese military doctrine is steeped in deception, the strategem is confined to closed societies and is incompatible with Western ideals of chivalry.[11] '*Maskirovka*' [12] certainly remains at the heart of FSU military doctrine and all FSU-trained staff officers are fully grounded in its principles:[13] witness the Serb employment of deception in 1999 against the North Atlantic Treaty Organization (NATO) in Operation ALLIED FORCE (OAF) [14] and Iraq's operational and tactical deceptions in the 1991 Gulf War. In addition to military activity, however, instances of strategic financial deception abound. For example, in 1994, Mexico achieved global economic surprise when she devalued the peso and totally deceived the International Monetory Fund.[15] These Western examples prove that open societies are fully capable of employing deception together with the commensurate operational security (OPSEC).[16] Military and financial environments share a common problem relevant to deception: it is not the lack of information that is the problem but the torrent of data polluted by misinformation.[17]

…the UK conducted operational deception in support of the San Carlos landing in the Falklands Conflict

If any society has the potential to deceive, how has the changing nature of conflict affected the utility of deception? Recent developments in the political and international security system, including the growth of Coalition operations, have certainly had an effect. With the demise of the bi-polar Cold War global structure, Western focus moved away from general war to Operations Other Than War (OOTW) such as limited or regional conflicts, COIN, counter-terrorism [18] and a new genre of operations, Peace Support Operations [19] (PSO), that are motivated by humanitarian interests. Peacekeeping (PK) operations have been conducted under UN auspices, often within a Coalition, with UK forces involved in the Former Republic of Yugoslavia (FRY) in Bosnia-Hercegovina (1995) and Kosovo (1999). Current doctrine suggests that deception may be employed to support appropriate PSO [20] especially in Peace Enforcement (PE) operations that employ coercive force.[21] However, it may not be applicable in every PSO, particularly PK when the need for transparency is paramount [22] and its use was expressly forbidden in Bosnia-Hercegovina.[23] The nature of Coalition operations also presents difficulties given the need to develop joint and combined deception doctrine and gain consensus for its use.[24] Finally, the nature of the adversary has altered and 'rogue' states and non-state actors (terrorist groups or ethno-nationalist factions) now pose an asymmetric threat. The viability of using deception against an asymmetric adversary [25] may be undermined by his diffuse command structure.[26] Such an adversary may also lack either the intelligence organization or the technological assets required to detect the signals of the deception plan. Furthermore, there is the problem of progressing a psychological and cultural analysis across a range of increasingly diverse adversaries to reveal potential deception avenues.

With the demise of the bi-polar Cold War global structure, Western focus moved away from general war to Operations Other Than War…

The above discussion has established a broad perspective from which to advance to the technological focus of this study. The past decade has witnessed the introduction of novel military technology with respect to the Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) force elements. Returning to the opening quotation, ISTAR is the sensory system that has created a more transparent battlespace for those who either employ it or who have access to its products; therefore, some believe that it renders deception transparent and worthless. This treatment ignores several issues: the linkage between battlespace transparency and its physical characteristics, the interpretation and limitations of the ISTAR product (which itself may have been 'deceived' through camouflage or signal manipulation) and the essence of strategic and operational deception. Significantly, it also ignores the psychological mechanisms of deception and the fact that these work through human beliefs and perceptions. The second technology-related issue has been the growth in real-time media reporting from the battlespace. In many respects the media may be considered to form an element of the battlespace sensory system. They are now able to disseminate information potentially critical to all levels of

…the media may be considered to form an element of the battlespace sensory system

war in real-time and this could undermine friendly deception plans. In addition to the key factors to be considered, 3 more concerns for the future utility of deception will be mentioned here for completeness. Firstly, deception operations must be planned by a dedicated staff to ensure that planning at all levels is synergistic [27] but further work within the UK is required at the strategic level.[28] Secondly, another reason for the relative paucity of UK deception could be a general lack of awareness of past deception success and the tangible value of the strategem. In the era of constrained defence expenditure, should not any force multiplier be exploited to its utmost? Thirdly, ambiguity exists concerning the legality of some acts of technological deception that, in future, may be constrained by International Law.[29] No apology is made for leaving these final issues undeveloped as such 'enablers' must receive attention once the case for deception in the modern battlespace has been conclusively made. Turning now to the scope of the paper, it must first establish a basis from which the ISTAR and media aspects can be analysed. It will describe what is meant by deception, review its doctrinal foundation and outline its meaning at the strategic and operational levels. The mechanisms through which deception works will then be explored together with an illustration of its quantitative value. Before presenting an overview of the ISTAR and media issues, battlespace characteristics will be considered. Finally, ISTAR and media aspects will be analysed within the security constraints imposed by this paper. The military-media relationship and the ethical considerations of employing the media in deception operations will not be studied in detail. Although some psychological aspects will be described, a detailed study of decision-making theory is outside the scope of this paper. The efficacy of deception will be illustrated by brief references to relevant case studies.

WHAT IS DECEPTION & WHY EMPLOY IT?

Sun Tzu identified the key starting point for any deception plan – understanding the enemy's innermost thoughts

Deception is designed to mislead the enemy and to induce him to act in a manner prejudicial to his interests.[30] Deception is most effective when used to attain surprise: for example, the prosecution of a friendly CoA disguised by deception will surprise the enemy. Deception has been attractive as a force-multiplier and to gain surprise, but it has never been seen by strategists to be a principle of war in its own right.[31] Sun Tzu and Clausewitz held differing opinions on the efficacy of deception. Clausewitz considered surprise to be difficult to achieve and that deception was almost always a waste of resources [32] but he also recognised its value under specific circumstances: 'the weaker the forces are ……the more appealing the use of cunning becomes'. Clausewitz's opinion was a reflection of his time: the growth in size of military formations was not matched by improvements in communications and mobility, and this reduced the utility of deception.[33] Sun Tzu valued deception as a force-multiplier and it is the most frequently discussed theme in the '*Art of War'* with emphasis placed on employment at all times and at all levels of war.[34] Sun Tzu identified the key starting point for any deception plan – understanding the enemy's innermost thoughts.[35] Manoeuvrist operational art identifies potential enemy centres of gravity to be cohesion and the 'will to fight' and both can be undermined by surprise generated by deception.

Strategic deception is a national or governmental concern;[36] the working assumption is that it seeks to portray a false CoA and mask military intentions at either the Grand or Military Strategic levels in order to serve national or governmental objectives.[37] UK doctrine for strategic deception remains to be developed [38] but it will be an element within the Information Campaign (IC), the over-arching plan involving Government departments and agencies. The military task within the IC will be Information Operations (IO) that must reach down through all levels of war to ensure synergy and unity of purpose.[39] IO is divided into Offensive and Defensive IO and deception is placed within Offensive IO (OIO), the aim of which is to alter the perceptions of decision-makers. The NATO strategic definition is that 'an adversary should be misled about the time, place, strength and nature of intended Allied Joint Operations';[40] however, NATO has yet to identify a co-ordination mechanism to obtain strategic political and military consensus amongst the 19 nations.[41] Operational deception must complement strategic deception and will be conducted in support of an operation or a particular phase of operation.[42] NATO doctrine states that operational deception should be planned at the Joint Force Headquarters (JFHQ) level and should 'mislead the adversary about the conduct of operations'. [43]

NATO doctrine states that operational deception should be planned at the Joint Force Headquarters (JFHQ) level and should 'mislead the adversary about the conduct of operations'

Having described the developing doctrinal foundation for deception together with some working definitions, how does it work and can success be quantified? Deception sets out to create and maintain a lie and most successful deceptions reinforce or capitalise on the enemy's existing perceptions: because of this, deceptions almost never fail and surprise is often inevitable.[44] Real events are used to reinforce the deception whenever practicable:[45] 'the lie…..was so precious that it should be flanked with an escort of truths'.[46] As presaged by Sun Tzu, deception occurs inside the brain of the person deceived.[47] The primary target is the adversary's intelligence organisation (his sensory system) that produces the supporting analysis for the military decision-maker and monitors the plethora of 'channels' of information through which signals (data) are received.[48] Information can be received from the media, ISTAR assets (including surveillance sensors and means such as electronic, signals and communications intelligence (ELINT, SIGINT, COMINT)) and human intelligence (HUMINT). Analysis of the data reveals the status of the adversary and will influence the assessment of his CoA. Through manipulation of signals, the aim of deception will be to steer the enemy's analysis to arrive at the desired (but wrong) CoA. However, it will not be all plain sailing as the sheer volume of information can create 'noise' to mask the intended data. If the signal is received, it will be ranked according to the credibility of the source or channel.[49] Independently verifiable and credible information is critical to the success

of the deception: the enemy must work for the data.[50] Technical deception measures include the generation of false and genuine radio (or other data) traffic to generate noise and confusion.[51] Physical measures may also support deception through military exercises and troop movements, the use of dummy/decoy equipment and camouflage.[52] The deception must also be tailored to the target's character and indeed several Israeli deceptions failed because the data (bait) was not recognised by Arab intelligence;[53] this also illustrates that deception is more a creative act than an exact science.[54] The theory of *cognitive dissonance* is helpful to explain why deception and surprise are inevitable. A person selectively organises his ideas about persons and things based on a finite quantity of data that can be stored within his personal cognitive world. This world is shaped by his physical and cultural environment, his psychological structure, goals and past experiences.[55] Once the person has made a decision and chosen a CoA, the psychological situation changes: the theory holds that the individual experiences psychological discomfort when presented with conclusions that do not match his pre-existing cognitive structure.[56] He will be inclined to place less emphasis on objectivity, and partiality and bias intrude into the evaluation of alternatives.[57] Military history is littered with examples of dissonance and its costs are frequently high: Montgomery's decision to attack the 'bridge too far' at Arnhem was one example.[58] The significance of dissonance theory in the era of ISTAR technology will be revisited later but, to close this section, can the military value of deception be quantified? Developing IO policy recognises the need to measure the effectiveness of deception but acknowledges the difficulty in measuring the effects of OIO, and it observes that the absence of quantitative evidence may damage the credibility of the strategem.[59] In his study of 93 Western military battles from 1914-1967, Whaley found that strategic deception occurred in 76 cases. Whaley's data [60] revealed that, where present, surprise became steadily more reliant on deception and remained highly probable even in the face of warnings [61] or, in other words, the compromise of OPSEC. Deception is never the sole means to the operational end but it generates surprise, and what price surprise?

Physical measures may also support deception through military exercises and troop movements, the use of dummy/decoy equipment and camouflage

…Napoleon assessed the value of the 'psychological' factors of war to be 3 times the worth of material factors

Whaley estimated that surprise changed the ratio of casualties in favour of the attacker from 1:1 to 5:1 [62] and Napoleon assessed the value of the 'psychological' factors of war [63] to be 3 times the worth of material factors.[64] More recently, Admiral Ellis's conclusion following OAF considered that had IO (including deception) been better used, the conflict would have been shortened by one half.[65] Surprise increases the probability of a quick and decisive victory whether measured in terms of sought goals, ground taken or casualty ratios,[66] thus reducing the expenditure of time, effort, resources and casualties.[67] The ability to generate surprise will also depend on the characteristics of the battlespace, the developing nature of which will now be considered.

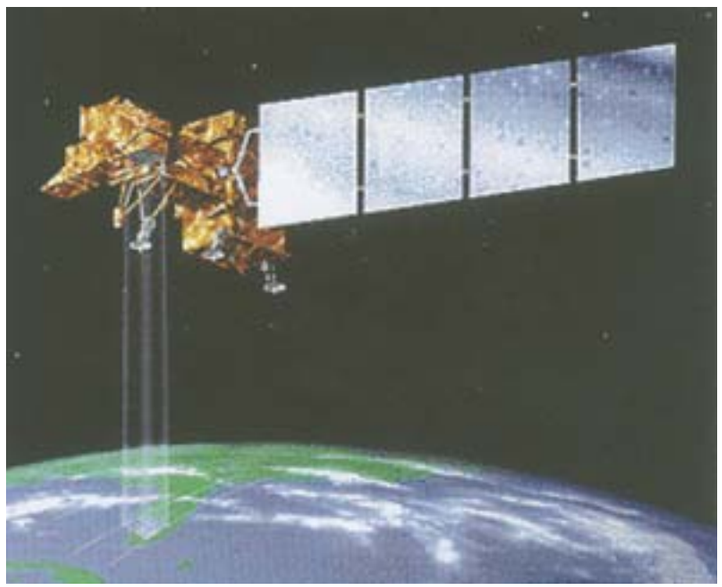
BATTLESPACE CHARACTERISTICS

The means to prosecute deception will depend upon the environment within which operations are conducted – the 'battlespace'. For example, to be effective, camouflage needs to match the environment, extremes of which are urban, jungle and desert. With the increasing urbanization of global society, urban operations in particular are expected to become more prevalent in future. Being filled with non-combatants and dense infrastructure, the urban environment has several unique characteristics: tall buildings, tunnels and sewers give the battlespace characteristics of height and depth that are absent on more open terrain.[68] Unique to the urban environment is the presence of many non-combatants [69] who affect operations: non-combatants acted as couriers in the Egyptian defence of Suez City, for example.[70] In the urban environment, the utility of deception is enhanced for several reasons. Firstly, the physical reaches of deception in the urban geography are increased through the multiplicity of surface spaces.[71] Secondly, no operational environment is 'noisier' and the glut of ELINT, COMINT and SIGINT signals may be masked by the noise generated by non-combatants and commercial activity. Deception can exploit the high level of 'background noise' and confusion, given a high level of coordination and oversight.[72] Thirdly, decision-making tends to be hastier and less well-informed in the urban environment as urban operations feature degraded C2, stress and high operational tempo.[73] Finally, and of most significance to this study, urban clutter blunts the efficacy of current ISTAR technology due to infrastructure masking, electronic noise, interference and propagation difficulties and erodes any technological advantage enjoyed by superior forces.[74] The overall effect on the prosecution of deception is that the number and power of the intelligence channels available to the target are reduced, albeit that HUMINT and media sources may increase for the party on home (urban) ground. Conversely, the friendly ability to analyse a target's CoA will be subject to noise and confusion and may enjoy minimal ISTAR support. Deception at the operational level was successfully employed in the high-intensity, major theatre urban

conflict of the Chechen defence during the Battle for Grozny in Jan 95.[75] Deception was employed at all levels of war to both entrap the Russians and to force protect. The background noise was increased because the city was in complete chaos and there were many urban resources available to be exploited for deception (news media, civil communications and HUMINT).[76] Having now laid the foundations of the strategem of deception, and illustrated the significance of battlespace characteristics to its employment, the specifics of ISTAR and real-time media reporting will be detailed.

ISTAR TECHNOLOGY & BATTLESPACE MEDIA

The continued utility of deception in the face of technological progress was first questioned in 1905 when it was believed that the vastly improved means of information dissemination following the introduction of the telegraph would eliminate surprise on a large scale in warfare.[77] However, once the telegraph was exploited to send deceptive signals, the technological tables were turned. Developments in ISTAR capabilities that make the battlespace more transparent at the strategic and operational levels include surveillance and electronic signals intercept sensors carried on a variety of airbreathing and non-airbreathing airborne platforms and ground-based collectors. To concentrate first on satellite-borne equipment, ISTAR imagery intelligence (IMINT) data for surface surveillance may be collected from electro-optical (EO) equipment across the electromagnetic spectrum (from the ultra-violet (UV) to the infrared (IR)) and wet-film photography retains value on many platforms. Radar is also used for air, maritime and ground surveillance: high resolution ground surveillance is conducted using synthetic aperture radar (SAR) that utilises the motion of the platform to synthesize an apparently larger-than-life sensor aperture. Signals intercept equipment provides a real-time feed of mainly military ELINT (but with some COMINT and SIGINT capability) and the sensors are generally cheaper and capable of collection over a much larger geographical area those collecting IMINT. The targets for COMINT, ELINT and SIGINT include all military and political communications, and the electronic characteristics and location of equipment.[78]



Landsat Satellite

During the Gulf War, commercial satellites, particularly the LANDSAT and French SPOT series, were used to support Coalition activities

The West enjoys a superior information position over many potential adversaries with its ability to collect, process, protect and distribute timely and accurate ISTAR products. Future concepts envisage all ISTAR platforms linked into a system of systems architecture that will encompass national, theatre and tactical sensors.[79] The US, in particular, has made significant progress towards the next generation of military satellite imagery but she also encourages the use of commercial assets. Satellite remote

sensing is expensive not only because of the launch and payload but also that 90% of the expenditure is needed to support data exploitation;[80] therefore, a vibrant market for high-resolution imagery has developed.[81] Such imagery was previously controlled by the US and Russia but commercial realities have created the potential for quality imagery to be available on demand by potential aggressors.[82] During the Gulf War, commercial satellites, particularly the LANDSAT and French SPOT series, were used to support Coalition activities.[83] To have true intelligence value, a discrimination of 1m Ground Sample Distance (GSD) or less is required, although 3m GSD sensors can determine the general presence of military equipment. Currently only a limited number of sources possess high-resolution equipment but the first commercial satellite, IKONOS, was launched by 'Space Imaging' in Sep 99 [84] and the first in a constellation of 8 EROS satellites (0.8m resolution) was launched in Dec 00 by the Israeli company 'ImageSat'.[85] Japan plans to launch the 2.5m GSD Advanced Land Observing Satellite (ALOS) in 2003 [86] and India, Brazil, China and Germany have the potential to develop similar systems: Germany has approved the supply of a 2m GSD satellite to Taiwan. France appears more reticent about the supply of high-resolution images [87] and the HELIOS 1A satellite was developed as an independent surveillance capability. Although not as capable as current US military imagery, its successor (HELIOS-2) will employ a 50cm GSD sensor.[88] With an expanding choice of suppliers, potential client states such as Iraq and Libya may find a willing supplier [89] but customers must wait for their tasking to be undertaken [90] and the timeliness of the data is subject to orbital dynamics and satellite constellation size. Constant surveillance is not possible away from the equator and even satellites with an oblique viewing capability such as SPOT require to re-visit equatorial latitudes every 3-4 days,[91] customer priority notwithstanding. The main frustration for customer states could be that commercial, high-resolution satellites may be subject to national Government monitoring and intervention. For example, LANDSAT continued to sell imagery throughout the Gulf War 1991 but the 30m resolution was too coarse to provide significant intelligence to Iraq. SPOT imagery (10m) was restricted to customers with Western military security clearances but Russian Soyuz-Karta images (5m GSD) were available on the open market although with restrictions intended to preclude transfer to Iraq.[92] Prior to the war, Iraq had purchased 20 SPOT photographs of Saudi Arabia and Kuwait with the final delivery made on 2 May 90.[93] There was speculation that Russia provided information on the timing of US satellite overflights; however, it would appear that no satellite imagery of the VII Corps western flanking manoeuvre was passed to Iraq.[94] US Space Command's vision for 2020 acknowledges the concern that the growth of multinational satellite-operating conglomerates may frustrate regulation and, therefore, active measures may be required to deny satellite products to adversaries.[95] Potential denial measures include the use of microsatellites to 'block' the sensor's view and communications jamming or disruption of the controlling ground segment. Destructive anti-satellite (ASAT) measures are also under consideration: the Chinese tested a high-power ASAT laser in 1999 and Russia is believed have a similar capability.[96] Compared to EO sensors, SAR satellites such as the US LACROSSE are large [97] and expensive to launch; therefore, commercial satellite SAR resources are currently limited in number and resolution (8m, adequate for ship

With an expanding choice of suppliers, potential client states such as Iraq and Libya may find a willing supplier…

classification) [98] although 3m resolution or less is anticipated.[99] ELINT, COMINT and SIGINT satellite products remain currently within the military domain.

Moving now to airbreathing and ground-based assets, air and maritime surveillance can be conducted from platforms such as the E3 Sentry Airborne Warning and Control System (AWACS – employed by NATO, US, UK and France), ground-based radars and the Nimrod MR2 and P3 Orion maritime patrol aircraft. Airborne and ground-based collection systems cover a wide range of ELINT, SIGINT, COMINT and Measurement and Signals Intelligence (MASINT) activities. As for ground surveillance, the US Joint Surveillance Target Attack Radar System (JSTARS) is capable of SAR surveillance to 250 km and, using Moving Target Indication (MTI) radar, can locate and differentiate between tracked and wheeled ground vehicles.[100] The UK Airborne Stand-off Radar (ASTOR) will offer a similar capability to JSTARS as will the Advanced SAR improvement on the U2.[101] SAR and MTI are expected to the carried on future Uninhabited Air Vehicles (UAV) that have been employed since the Vietnam and Yom Kippur Wars [102] and the US PREDATOR already carries SAR and IR sensors. Current UAVs are much cheaper than radar and EO surveillance aircraft and their COMINT, SIGINT, ELINT and MASINT counterparts (RIVET JOINT, Nimrod R1 and COBRA BALL). All ISTAR aircraft are extremely high value assets and, consequently, are relatively few in number: the unit cost of JSTARS is $225 million, for example.[103] Given the cost and sophistication of most ISTAR technology, how much of it is available to potential adversaries through proliferation and do indigenous capabilities exist? Before the end of the Cold War, many 'Third World' states enjoyed rapid economic growth and were able to acquire sophisticated technology. The most spectacular growth was in the Pacific Rim [104] and, despite the Asian economic crisis in 1997-98, China, Singapore and Taiwan remain well placed to purchase.[105] The supply of technology to more threatening potential adversaries (Libya, Iran and Iraq) is largely constrained by embargoes but the future of these is unclear.[106] The US and Russia have increased their exports of military technology: Moscow needs arms exports for hard currency and to maintain jobs. The Russian arms-exporting company *Rosvoorouzhenie* [107] has adopted an aggressive sales policy to China, Iran and Syria, and Iraq is a long-term Russian ally. The success of AWACS has prompted orders for the next generation Boeing 767-27C AWACS for Japan, and Australia has ordered 4 AWACS 737-700 aircraft.[108] Sweden have developed an indigenous AWACS capability based on the SAAB 340 and the Ericsson 'Erieye'

The Russian Beriev A-50 'Mainstay' provides an airborne control and surveillance capability, albeit not as sophisticated as the AWACS

radar, and Ericsson have teamed with Embraer (Brazil) to produce 5 surveillance aircraft to contribute to the Amazon Surveillance System.[109] Israel developed the 'Phalcon' surveillance system capable of detection out to 400km in a Boeing 707 airframe that was bought by Chile and China and offered to North Korea.[110] The Russian Beriev A-50 'Mainstay' provides an airborne control and surveillance capability, albeit not as sophisticated as the AWACS. In April 2000, Russia reached a preliminary agreement to lease 2 A-50s to India, and Rosvoorouzhenie is reported to have entered negotiations with China for the Phalcon replacement.[111] Iraq was known to possess an indigenous AWACS programme but the doubtful capabilities of the ADNAN 1 (sensor unknown) and the BAGHDAD 1 (utilises the Thomson-CSF Tiger ground-based radar) were never brought to bear in the 1991 Gulf War.[112] Although AWACS technology has spread, there is little evidence of widespread proliferation of the more sophisticated SAR and MTI and it is unlikely that rogue states could spring much technological surprise on the West given the cost and technological complexity. However, as with satellite imagery, strategic and operational intelligence support (ELINT, COMINT and SIGINT) may be available from a third party state augmented by ground-based ISTAR equipment which may lack wide geographical coverage but is more readily available. So much for ISTAR in isolation, what now about the effects on deception of the second technologically-driven factor, the real-time media?

Media reports were first filed from the battlespace in the Crimean War but today the ever more pervasive and instantaneous media presence means that tactical acts may achieve strategic significance.[113] How does this real-time presence affect strategic and operational deception? The inescapable tension between the need for OPSEC and press freedom was recognised in 1944 by Eisenhower: 'the first essential of operations is that no vulnerable information should go to the enemy…. The first essential in reporting is wide-open publicity'.[114] For study purposes, the 'media' comprise the modern, electronic international news media including TV, radio, wire services and major newspapers that is dominated by American corporations supplemented by a secondary British element. While the US Freedom of Information Act (1966) presumes a media 'right of access', European Governments can employ a range of secrecy laws to contain information;[115] however, the direct censorship commonplace in most parts of the world is only used in the most extreme circumstances in the West.[116] The idea of excluding the media from an area of conflict has become legally doubtful and increasingly difficult over the last decade.[117] Given the freedom of the western media it is not difficult for potential aggressors to gain information on military capabilities, and corporations such as CNN may well have teams employed on both sides of the conflict and could, theoretically, act as intelligence sources for both sides.[118] When deception is being attempted, therefore, media knowledge of either the deception or the real operational plan could be highly dangerous.[119] The media have the potential to compromise deception-generated surprise in 2 ways: either through the innocent reporting of the facts of the plan or through detached and impartial analysis, revealing strategic options to the enemy.[120]

To add a measure of perspective, however, not every military operation attracts media interest. Some media have both limited resources and a low interest threshold: the slow pace of events in Bosnia proved incompatible with the requirements for a good

TV story.[121] The British-led COIN operations in Oman (1970-75) attracted little interest whereas the US marine landings in Somalia (1992) occupied the opposite end of the spectrum. Although censorship is rarely used, methods may be employed to control the press but, in future, this will very much depend on the specifics of the operation. In the relatively inaccessible environment of the Falklands Conflict, only a very small number of journalists were permitted to travel with the Task Force. Although officially there was no Government censorship, many topics were inadmissible from the outset; furthermore, journalists were largely reliant upon military communications.[122] By contrast, in the 1991 Gulf War, access to Saudi Arabia was relatively straightforward. The media had become more mobile and self-sufficient, equipped with lightweight camcorders, portable editing suites and satellite communications.[123] Control was employed through a media 'pool' that offered journalistic facilities, including membership of select Media Reporting Teams (MRT) in return for the acceptance of limitations, although many editors demanded strict adherence to the rules out of patriotism.[124] Patriotism was not so evident when the US deployed to Haiti (Op JUST CAUSE) and several hundred journalists, including 8 CNN crews, preceded the US deployment despite the President's request for a voluntary news embargo.[125] Such an action illustrates the media's potential to undermine the OPSEC associated with an operation or strategy but, in contrast, OPSEC was maintained when the MRT journalists were briefed about the DESERT STRIKE battleplan in advance.[126] Turning to the compromise of strategy, there was open media speculation about potential Coalition strategy before and during the 1991 Gulf War. Many broadcasts discussed the potential for the American and British flanking manoeuvre [127] and on 11 Feb 91, *Newsweek* published a map that, Schwarzkopf recalled, 'almost exactly depicted our flanking plan'. Iraq obtained little intelligence from her very limited ISTAR assets and used the BBC, Radio Monte Carlo and CNN as her main sources.[128] Despite the potential compromise of strategy, however, Iraq seemed to draw little to inform her analysis about the Coalition's intentions.[129] Nevertheless, media speculation about newsworthy conflicts must only increase in the future given the ever-growing 24-hour news industry. With the volume of media-generated information set to increase, the trend for large numbers of journalists to be present will continue, fuelled by the absence of travel restrictions. Many agencies employ fiercely ambitious and cheap 'stringers' (freelance journalists) who are eager to make their reputations and who pay little regard to the restrictions and dangers of the theatre. Forty journalists were captured by the Iraqis in Basra during the Gulf War, a small number of British, French and US 'unilaterals' reported from within Iraqi-held and restricted Saudi territory,[130] and an estimated 49 journalists were killed during the early fighting in Yugoslavia in

In the relatively inaccessible environment of the Falklands Conflict, only a very small number of journalists were permitted to travel with the Task Force

1993.[131] In addition to the presence of unaccredited journalists, the level of military control may be further undermined in PSO given that UN forces have been forbidden to provide press facilities as this would imply a degree of unacceptable bias.[132] The increasing ease with which information can be disseminated from the battlespace has the potential to give the adversary advance information on troop concentrations or manoeuvres about which he may have been unaware. Information disseminated from the non-accredited and uncontrolled media poses the worse danger.

ISTAR, MEDIA & DECEPTION

…Israel and the US were totally surprised by the Egyptian assault on 14 Oct 73…

The above discussion has examined some key factors of ISTAR and media reporting and it is now necessary to analyse how they affect the employment of strategic and operational deception. How transparent has the battlespace truly become to both friendly forces and potential adversaries, through the use of ISTAR, and does deception still have a role in strategic and operational art? With respect to the media, can deception be sustained following the compromise of OPSEC, and is harm done by open media speculation about friendly CoA? Finally, does the real-time impact of media reporting and some ISTAR assets have the potential to unseat a strategic or operational deception plan? To recap, although doctrine at the strategic level is being developed, strategic deception should seek to mislead about military and political objectives while operational deception seeks to mislead about the conduct of the military campaign or a phase of operation. Both seek to have the adversary determine the wrong friendly CoA – deception must help him to be quite certain, decisive and wrong![133] Deception works through the psychology of misperception [134] and seeks to confuse the target so that he is unsure as what to believe or to mislead him by building up an attractive view of the wrong alternative.[135] Some illustrative detail has already been described and 2 further case studies will be employed. Firstly, OAF (1999) as it exemplified successful operational deception in the face of overwhelming ISTAR superiority. Secondly, the Egyptian strategic and operational deception in advance of the 1973 Yom Kippur War, because it occurred despite Israeli ISTAR advantage and Egyptian media compromise of OPSEC.

Turning first to OAF, despite extremely high levels of the most sophisticated Allied ISTAR tasking, coalition targeting and surveillance were frustrated by relatively simple deception techniques. For example, military logistics and armoured vehicles were moved at the same time as refugee columns: JSTARS could discriminate between tracked and wheeled vehicles but not between military and civilian tractors and trailers.[136] A fatal misidentification occurred at Djakovica when Serbia alleged that 75 civilians were killed and NATO admitted to targeting ‘military’ vehicles and hitting 2 convoys.[137] Through tactical measures of camouflage and concealment, the Serbs achieved operational deception with respect to the number of items of military equipment destroyed. NATO claimed that 60% of the Serb artillery and 40% tanks were either damaged or destroyed; however,

the NATO assessment team revised down the initial figures of 449 artillery and mortar pieces to 389, and only 3 damaged T55 tanks were found in Kosovo.[138] Moving now to the Yom Kippur War, the surprise generated by the Egyptians provides an excellent example of the triumph of cognitive dissonance in the face of apparent hard fact. Israel knew about the build-up of forces on the Egyptian side of the Suez Canal from US intelligence, electronic surveillance, photography from the US SAMOS satellite and HUMINT.[139] Despite this, Israel and the US were totally surprised by the Egyptian assault on 14 Oct 73 but, as Kissinger stated: 'Nobody made any mistakes about the facts'. Following the Arab defeat in the 6-Day War (1967), Egypt had re-equipped and re-organised her armed forces with Russian assistance and many call-ups of reservists and deployments along the Suez Canal were conducted. The partial Israeli mobilizations in response were so frequent that the likelihood of war was undermined because no military action followed the Egyptian call-ups, in effect Israel was conditioned to ignore the preparations for war.[140] In May 1973, the CIA obtained the Egyptian plan of attack for Yom Kippur but failed to believe that the scheme was serious.[141] Closer to the attack, the Cairo-based Middle East News Agency reported the Egyptian 2nd and 3rd Armies to have been put on alert on 2 Oct 1973.[142] President Sadat kept the invasion date secret, the build-up was assessed as another 'demonstration' and the strategic surprise on 14 Oct 73 was complete. As described theoretically in an earlier section, decision-making requires a set of hypotheses about the enemy against which to test all the received signals. The cultural barrier between Arab and Israeli affected the analysis and cognitive dissonance prevented an objective view being taken of many signals including those from ISTAR and the media. Following the Arab defeat in 1967, Israel had been conditioned to believe in her superiority and, in 1973, could not envisage that the climate was right for an Arab assault. The Arabs were willing to risk military defeat to improve their political position and the Israelis were unable to anticipate this behaviour.[143] The evidence from the Yom Kippur War tends to reinforce Whaley's statistical conclusion that high-level deception is almost always successful regardless of the sophistication of the victim.[144]

ISTAR technology has certainly enhanced the ability of those enjoying access to its products to gather large quantities of data about the adversary and seed the analytical process. The 2 case studies show that analysis must not merely concentrate on capabilities: the adversary's *intentions* are required to determine the most likely CoA, particularly at the strategic level where the CoA might be hidden within the mind of the decision-maker. The difference between the levels is seen in the CoA – *the decision to use military force*, rather than the more

The evidence from the Yom Kippur War tends to reinforce Whaley's statistical conclusion that high-level deception is almost always successful regardless of the sophistication of the victim

tangible operational CoA, the detail of an invasion plan or operational phase – the *where, when and how?* Intentions at these higher levels are difficult to observe directly and must be inferred. Even observed operational movements and concentrations require objective analysis: are they localised tactical manoeuvres, feints to generate future complacency, or the first operational strokes on a masterpeice to be created through operational art? ISTAR IMINT assets are particularly useful to gain tactical or operational information on capabilities and concentrations but COMINT may come closer to revealing intentions. However, information must be credible and the enemy must work for it: he might 'collect' the real battle plan but if ignored by the (human) analyst, the real CoA may remain masked. Acceptance of manipulated data, the presence of cognitive dissonance and the sheer volume of data all influence the analytical process. Deception at the higher levels has an opportunity to succeed in the face of the most sophisticated technology because of the requirement for the CoA to be inferred through the human cognitive process. Aside from this, ISTAR platforms possess technological limitations that could undermine the credibility of their data and their operational features could be exploited to deny or frustrate success: surveillance should be undertaken only with the full consciousness of the likelihood of deception.[145] Firstly, assuming credible ISTAR data, there are several obvious operational weaknesses that undermine ISTAR's seemingly ubiquitous power. ISTAR assets are vulnerable to the effects of the adversary's counter-surveillance effort.[146] Space platforms may be denied through passive or ASAT measures and they have predictable orbital characteristics that can be exploited to plan movements of men and matériel. Furthermore, space IMINT is not available instantaneously and EO sensors will be denied by poor weather: evidence from the 1991 Gulf War suggests that 3 days were required to revisit the complete range of targets and up to 18 hours elapsed between collection and the image reaching the analyst.[147] Air-breathing platforms are vulnerable to high value asset attack (HVAA) to either destroy the platform or to force it from the tasked surveillance area. For example, due to Coalition air superiority in 1991, Iraq was unable to employ her very limited airborne EO and SIGINT/COMINT capabilities.[148] Less vulnerable to HVAA and more numerous are the UAVs, but they are currently less capable than manned aircraft (although UAV replacements are being considered for AWACS and JSTARS). The conclusion is that only limited volumes of battlespace may be transparent at any instant, given the relatively small numbers of ISTAR assets and their operational limitations. Secondly, the credibility of ISTAR data can be undermined by technological or topographical means. Surveillance of the Warsaw Pact's invasion of Czechoslovakia (1968) was hidden by jamming and anti-radar chaff [149] and, while the technological resilience of modern ISTAR sensors has improved, such measures cannot be ignored and were successfully employed in OAF. Camouflage remains a potent counter-ISTAR technology that can defeat UV, visual, IR, thermal, photographic and radar sensors:[150] a multi-cornered metal reflector can mimic a tank on SAR, for example.[151] The employment of counter-ISTAR camouflage against adversary ISTAR will be vulnerable to 'eyes on' adversary HUMINT, the prevalence of which will depend on the battlespace characteristics.[152] Finally, ISTAR performance is degraded by battlespace topology. Mountainous or jungle terrain and the structural and human characteristics of the urban environment are especially difficult to penetrate with ground surveillance assets. An asymmetric enemy could draw conflict into areas where ISTAR technology is degraded to support his own deception measures. Saddam Hussein could, for example, have chosen to fight in Kuwait City rather than on the desert terrain that favoured

the Coalition ISTAR.[153] ISTAR's vulnerabilities are often forgotten and too much faith can be placed in the infallibility of technology.[154] In WW2, the Germans' absolute faith in the cryptographic technology of Enigma resulted in their being deceived, and electronic or physical spoofing applied to JSTARS or ASTOR could have a similar effect.[155] Data saturation is an especially significant problem in the modern era with the multiplicity of data sources, especially with respect to SIGINT/COMINT/ELINT, and analysts need to be selective to avoid being overwhelmed. Giving the most weight to the most prestigious ISTAR asset is also problematic as the deceiver could target this as a priority. In the future intelligence 'systems of systems' may counter this and all-source data will be impartially integrated into a coherent picture by software algorithms,[156] not the dissonance-susceptible, over-loaded analysts. The integration algorithms may have a human designer, however!

Having first looked at ISTAR, what are the effects of media reporting from the battlespace? The successful deception during the 1991 Gulf War and experiences such as the compromise of OPSEC before the Yom Kippur War show that deceptions have worked despite media CoA speculation and the compromise of OPSEC.[157] Deception works by reinforcing the adversary's beliefs: Iraq expected the Coalition to launch an amphibious assault and Israel did not expect Egypt to go to war. However, would the deceptions have worked had ISTAR served to corroborate the data received from the media? In the 1991 Gulf War, the Iraqis were reliant on the media as a main source of information and they lacked detailed information on Coalition force concentrations. The heavy media coverage of the US Marine Corps' training suggested the amphibious landing in Kuwait to be the most likely CoA, thus masking the true CoA, the western flanking manoeuvre of VII Corps. ISTAR products showing the VII Corps assembly areas could have alerted the Iraqis to the real CoA and given some credence to the alternative media speculation about the flanking manoeuvre. However, analysis is a critical part of the process; for example, in 1973 the Israelis had substantial ISTAR resources to observe the build-up of forces but the analysis apparently ignored ISTAR products and the corroborative media alert. In addition to ISTAR and other signals, the media present one more element in the analysis burden. The relative value of media sources is difficult to gauge but, largely, the relative standings of the accredited, 'controlled' journalist and the unaccredited, 'uncontrolled' stringer is marginal to the argument because deception is a 'need to know' subject about which journalists will not be briefed. While material from accredited journalists may attract a greater weighting in analysis, the pertinent issue is the credibility of the information. Intelligent

In WW2, the Germans' absolute faith in the cryptographic technology of Enigma resulted in their being deceived, and electronic or physical spoofing applied to JSTARS or ASTOR could have a similar effect

speculation may be helpful to an adversary, particularly one from a different culture, but non-democratic aggressors may treat any media information with caution given that they use the media to perpetuate deception themselves. Although this is considered unethical in the West,[158] during the Battle for Grozny (1995), the Chechens used the media for a strategic level disinformation campaign that presented a prejudicial view of the Russians and was also used to target the neighbouring Republics in an effort to widen the war.[159] Ultimately, intelligent media speculation is not hard fact and the enemy's analysis will include his own speculative thoughts; the media effect will be to add further subjectivity to the process.

A strategic deception which may span months or years of preparation will not be undermined by real-time and localised snippets of media data…

Finally, real-time media reporting can deliver a more immediate effect than most ISTAR platforms, especially when compared with the example of the 3-day 1991 Gulf War strategic IMINT cycle. A tactical action may have strategic effect in that the media may reach a target audience before the military chain is able to report. However, it is likely that the real-time media feed will come from a relatively localised area dictated by prevailing security conditions (from where it is acceptably safe to report or from where media access is permitted) together with the resources of the media corporations. In parallel, real-time ISTAR assets such as JSTARS are also relatively localised in their surveillance areas by sensor performance and the number of platforms. Again, this reinforces the view that only specific volumes of battlespace may be potentially transparent at any instant. At worst, the media may broadcast information on movements or concentrations of friendly force about which the adversary may have been ignorant. This will enable him to react in some manner and it may reduce the friendly ability to achieve total surprise or it may undermine a tactical advantage. However, the information represents localised tactical data, and the adversary will have to relate its significance to the higher-level plan. Furthermore, he may be unable to act in time to take advantage of the tactical detail and any action not aligned to upsetting the real friendly CoA may be wasted effort: the tactical action reported on may have been a feint. A strategic deception which may span months or years of preparation will not be undermined by real-time and localised snippets of media data: by the time the journalists are reporting, the strategic deception plan should already have been successfully employed! On the operational side, the planning cycle currently looks up to 72 hrs ahead and throughout the battlespace. Compromise of the operational deception plan is also unlikely to be unseated by a localised real-time feed of media or ISTAR product.[160] What is observed or reported at the localised, tactical level represents a 'snap-shot' in time and space within a larger window of operational effort. The enemy analyst would have to infer the

…during the Battle for Grozny (1995), the Chechens used the media for a strategic level disinformation campaign that presented a prejudicial view of the Russians…

developing operational plan from an extrapolation of many ‘snap-shots’: while not impossible, the lack of a truly transparent whole battlespace, cognitive dissonance and the multiplicity of sources in the analytical process will intervene to ensure that operational deception remains viable.

Several significant factors affect the utility of strategic and operational deception in the modern battlespace. Changes in the nature of global security and military operations have caused a growth in OOTW, including PSO, and deception may not always have a place in support of operations in which total transparency is mandated. The rise of the asymmetric threat has illustrated the importance of understanding the adversary’s decision-making process to determine whether it is open to deception. However, while these factors are germane to the argument and work is required to develop UK policy at the strategic level, this analysis has concentrated on the technological factors of ISTAR and real-time media reporting. The heart of the matter is whether the twin aspects have rendered the battlespace, and thus any strategic or operational deception transparent. Do these developments evoke a return to Clausewitz’s era when the absence of deception was merely a reflection of the times? At the higher levels of deception, the answer is a qualified ‘no’.

The examination of the characteristics of the future battlespace revealed both a likely growth in urban operations and that this environment severely degrades the utility of current ISTAR technology. In the light of ISTAR’s current limitations both now and in the near future in the urban environment, anticipated developments in urban ISTAR technology were not examined because they will not affect the conclusions of the analysis. Western nations have been shown to enjoy a technological advantage over most potential adversaries although commercially available EO IMINT has the potential to narrow the gap in strategic and operational intelligence collection. The development of indigenous capabilities would be a major undertaking by most potential aggressors and technological surprise will be unlikely. Notwithstanding Western ISTAR technological superiority, all sensors and platforms are subject to limitations including counter-ISTAR deception, and this means that total battlespace transparency is currently unattainable. Regardless of its technological superiority, the West has, therefore, remained vulnerable to an asymmetric adversary’s deception as amply illustrated by Iraq and Serbia within the last decade. If an asymmetric adversary can deceive in the face of ISTAR superiority, the strategem must remain a valid CoA for the superior force. Of greater relevance to the higher levels of war, however, and setting aside ISTAR’s technological limitations, the underlying reason for deception remaining a viable strategem is the human decision-making process. At the strategic and operational levels, the CoA must be inferred from observation and analysis; this process will be influenced by factors such as the volume of information, its credibility and source, and the pervasive human condition of cognitive dissonance. No amount of ISTAR observation can uncover what is within the human mind: for example, in 1973 were the Egyptians exercising or preparing for war? Despite advances in technology, the human mind has become no less susceptible to deception, indeed, the increasing dependence on the automatic processing of increasing volumes of information may make it more vulnerable,[161] especially if the dependence favours an ISTAR sensor that is being deceived. At the strategic-level, the human processes can be expected to influence heavily the analysis of the CoA, as

demonstrated by the cultural and cognitive dissonance prevalent in Israel before the Yom Kippur War. Deception works to reinforce perceptions that may be immutable due to cognitive dissonance.

Analysis of the real-time media presence in the battlespace suggests that this is less of a problem to the viability of higher-level deception than may first have been thought. The media presence will only become more pervasive and less controlled in future, and will have some potential to disrupt operational level plans by inadvertent compromise of OPSEC or through informed speculation to reveal military options. However, although information from accredited journalists may attract some weighting in analysis, media speculation constitutes one more piece in the analyst's jigsaw, and a fairly intangible one at that. Evidence from the 1991 Gulf War illustrated the apparent lack of effect that open (and accurate) media speculation about the Coalition flanking manoeuvre had on the Iraqis, who lacked detailed ISTAR data. The more interesting area of study is the effect of real-time reporting upon the higher levels of deception and whether they would be undermined by the immediacy factor. ISTAR limitations, coupled with the human cognitive process, show that the battlespace is not fully transparent in real-time and a parallel is evident in real-time media reporting. It is certainly possible for instantaneous media reporting to cause tactical actions to have strategic effect; however, such reporting represents a 'snap-shot' in time and space, of clear relevance to the tactical level, but not of much significance to operational deception. The information presented may be detailed and accurate but, being media-sourced, it may carry little corroborative weight in the analysis. Furthermore, higher-level plans would have to be inferred from a series of fairly localised tactical observations. It is considered that the value of strategic deception will be unaffected by real-time media events and there may be a minimal effect at the operational level.

Overall, deception can succeed in the face of ISTAR superiority and the presence of media within the battlespace. Equally, the technologically superior force remains able to employ the strategem as can the adversary. Deception plans must continue to be developed to further operational art and to maximise economy of effort as historical experience illustrates that deception can reduce the cost of conflict. The FSU considers that it has not become too difficult to deceive in the face of ISTAR, it merely requires more resources and resourcefulness,[162] and planners have had the opportunity to see how exported systems fared against US-led Coalitions in the 1991 Gulf War and OAF. Such details will not have been lost on other potential adversaries. In this technological era, the serviceman needs to maintain a healthy scepticism about the true capability of ISTAR and an awareness of the potential of the media to act as a limited sensory system. Neither presents the silver bullet of full battlespace transparency. Neither will undermine the utility of strategic and operational deception while human factors are central to analysis. What the magician calls magic and the soldier calls deception remains a valuable tool of strategic and operational art.

BIBLIOGRAPHY

BOOKS & REPORTS

1. Buzan, B. '*Military Technology & Strategy*'. Macmillan Academic & Professional, 1987.
2. Carruthers, S.L. '*The Media at War – Communications and Conflict in the 20th Century*'. No publisher or publication date available.
3. Cobbold, R. '*An Acronym for the Millennium – ASR2*'. (in The International Security Review), RUSI, 2000.
4. Combelles-Siegel, P. *Target Bosnia: Integrating Information Activities in Peace Operations*. DoD CCRP, 1998.
5. Dailey, B.D. & Parker, P.J. *Soviet Strategic Deception*, Lexington Books, Hoover Institution Press, 1987.
6. Daniel, D.C. & Herbig, K. '*Strategic Military Deception*', Pergamon Policy Studies, 1982.
7. Davis, M. '*The RMA in Asia – The Stillborn Revolution*'. (in 'The International Security Review'), RUSI, 2000.
8. Dixon, N. '*On the Psychology of Military Incompetence*', Pimlico, 1994.
9. Greenberg, L.T., Goodman, S.E. & Soo Hoo, K.J. '*Information Warfare & International Law*'. DoD C2 Research Programme, National Defence University/CCRP, Jan 1998.
10. Handel, M.I. '*Masters of War: Sun Tzu, Clausewitz and Jomini*'. London: Frank Cass, 1992.
11. Handel, M.I. '*War, Strategy and Intelligence*'. London: Frank Cass, 1989.
12. Hughes-Wilson, J. '*Military Intelligence Blunders*'. London: Robinson, 1999.
13. Jane's Radar & EW Systems, 11th Edition 1999-2000.
14. Knorr, K. & Morgan, P. (Eds). '*Strategic Military Surprise: Incentives and Opportunities*'. Transaction Books, 1984.
15. Mason, T. '*The Aerospace Revolution*'. Brassey's 1998.
16. Sanders, D. '*Russia's Security* Challenge'(International Security in a Global Age (Jones, C & Kennedy-Pipe C (Eds)), Frank Cass, London, 2000.
17. Sawyer, R.D. '*Sun-Tzu, The Art of War*'. New York: Barnes & Nobles, 1994.
18. Whaley, B. '*Towards a General Theory of Deception and Surprise*' (In 'Military Deception & Surprise', Eds Gooch, J & Perlmutter, A.), Frank Cass, 1982.

PAMPHLETS & MILITARY PUBLICATIONS

19. ACSC4 Course Notes. ‘Media Operations’, Annex B to Serial 2, 2000.
20. *Allied Joint Doctrine*. AJP-01(A), Sep 1998.
21. *Army Field Manual*. Vol 1, Part 4, Oct 99.
22. Army Field Manual. Vol 2, Part 5, Issue 2, Nov 99.
23. Bayldon, R. ‘Op GRANBY – Deception in 1 Armoured Div’. D Sc(Land) Note for Record 12/92, 15 Jun 92.
24. *British Defence Doctrine*. Joint Warfare Publication 0-01. MOD-CS(M)G, 1996.
25. Burridge, B. ‘Defence & Democracy – The Control of the Military’, CDS Brassey’s, May 1998.
26. *Deception*. Joint Doctrine Pamphlet 2/98, MOD-CSE.
27. Dick, C.K. ‘Maskirovka in Yugoslav Military Thinking’. Conflict Studies Research Centre, A100, July 1999.
28. DISS Lecture Script. ‘Intelligence support to the IO Course’. Sep 1999.
29. Gewehr, S. and Glenn, R.W. ‘The Art of Darkness – Deception & Urban Operations’. RAND, 2000.
30. *Information Operations – A Policy Update*. MOD D/DTIO/300/1/1, 22 Feb 2001.
31. JPRS-UMT-91-006-L (Untitled). 18 Jul 91.
32. *Information Operations*. Draft Joint Doctrine Pamphlet XX-01, 1st Study Draft, JDCC, 1 Mar 2001.
33. Handel, M.I. ‘Perception, Deception & Surprise: The Case of the Yom Kippur War’. The Hebrew University, 1976.
34. *Op MASTIFF (Combat Ops After Action Report)*. MACV/RCS/J3/32. Dept of the Army, HQ 1st Infantry Div, 1966.
35. *Peace Support Operations*. Joint Warfare Publication 3-50. MOD-CSE.
36. RAF Manual: Air Operations.
37. *Techniques for Deception*. USACGSC RB 31-40. US Army Command and General Staff College, Fort Leavenworth, Jul 1974.
38. *UK Doctrine for Joint and Multinational Operations*. JWP 0-01, Edition 1. DSDC(L).

ARTICLES IN JOURNALS

39. Albright, D. ‘Masters of Deception: Trouble in the Gulf’. *Bulletin of Atomic Scientists*. May/June 1998, p44-50.

40. Duncan, A. ‘Mixing with the Media’. *British Army Review*. Aug 1995. p13-32.
41. ‘Concealment and Deception by Modern Camouflage Techniques’ (no author given). *Armada International*. No 6, 1986, p88-91.
42. Float, R. A. ‘Armed Forces & the Media: Improving the Relationship’, *British Army Review*, No 125, 2000. p83-95.
43. ‘Forging War: The Media in Serbia, Croatia and Bosnia-Hercegovina’ (no author given), *Article 19 International Centre Against Censorship*, Bath Press, 1998.
44. Glantz, D. M. ‘Surprise and Maskirovka in Contemporary War’. *Military Review*. Dec 1988, p51-57.
45. Handel, M.I. ‘Technological Surprise in War’. *Intelligence & National Security*. Jan 1987, p1-53.
46. Handel, M.I. ‘The Yom Kippur War & the Inevitability of Surprise’. *International Studies Quarterly*. Vol 21, Sep 77, p461-503.
47. Moorcroft, P. ‘CNN – The New Emperor of International Politics’. No publication given – ACSC4 Media Ops Reader.
48. Mueller, J. ‘The Perfect Enemy: Assessing the Gulf War’. *Security Studies*. No 1, Autumn 1995, p77-117.
49. Norman, W. ‘The Art of Deception’. *Aircraft Illustrated*. Dec 1997, p27-29.
50. Parker, R.R. ‘Deception: the Missing Tool’. *Marine Corps Gazette*. May 1992, p97-99.
51. Phillips, A.J. ‘UK Joint Deception Doctrine’. *Army Doctrine & Training News*. No 8, Nov 1999, p1-8 to 1-15.
52. Poynton, D.M. ‘Surprise can be achieved in war despite advances in EW & Surveillance Devices’. *Australian Defence Force Journal*. No 25, Nov/Dec 1980, p42-52.
53. Ralph, J. ‘Strategic Deception: the Anatomy of Success’. *War Studies Journal*. Spring 1996, p14-25.
54. Reading, R.W. ‘Could Iraq have made better use of its Air Force and Missile Technology during the Air War’. *Australian Defence Force Journal*. May 1992, p39-63.
55. Rothkopf, D.J. ‘The Disinformation Age’. *Foreign Policy*. No 114, Spring 1999, p83-96.
56. Savoie, T.A. ‘Deception at the Operational Level of War’. *Army*, Apr 1987, p30-37.
57. Stewart, R.A. ‘Strategic Intelligence: Barriers to Perception’. *British Army Review*. Aug 1989, p16-20.

INTERNET SOURCES

58. www.britains-smallwars.com (downloaded 14 Nov 2000)
59. www.earc.nasda.go.jp/alos (ALOS Satellite – Japan, downloaded 18 Feb 01)

60. www.fas.org/irp/congress/1996 rpt/ic21/ic21006.htm (Intelligence Community in the 21st Century (downloaded 21 Mar 01)).
61. www.fas.org/irp/program/collect/jstars.htm (JSTARS – downloaded 17 Feb 01).
62. www.fas.org/irp/program/collect/Predator.htm (Predator – downloaded 17 Feb 01).
63. www.fas.org/irp/program/collect/rivet.joint.htm (Rivet Joint – downloaded 17 Feb 01).
64. www.fas.org/irp/program/collect/imint/lacrosse.htm (Satellite IMINT – downloaded 17 Feb 01).
65. www.fas.org/man/dod-101/sys/ship/docs/98review/intelligence.htm (downloaded 30 Oct 2000)
66. www.fas.org/nuke/guide/russia/airdef/a-50.htm, Beriev A-50 Mainstay (downloaded 21 Mar 01)
67. www.fas.org/spp/guide/europe/military/weu/1643e.htm, WEU Assembly Report: Space Systems for Europe, 18 May 1999 (downloaded 21 Mar 01).
68. www.fas.org/spp/military/docops/operate/ds/images.htm (Desert Storm Military Space IMINT – downloaded 22 Mar 01).
69. www.fas.org/spp/guide/europe/military/weu/1643e.htm (Space Systems for Europe – downloaded 21 Mar 01).
70. www.fas.org/spp/guide/military/imint/helios1a.htm, Helios Military Observation Satellite (downloaded 21 Mar 01).
71. http://www.fas.org/spp/military/docops/operate/ds/images.htm (Desert Storm – Military Space Imagery Intelligence, downloaded 22 Mar 01).
72. www.c2b.hurlburt.af.mil/isrbm.htm (Intelligence, Surveillance and Reconnaissance Battle Management – downloaded 30 Nov 2000)
73. www.dtic.mil/execses/adr2000/chap8.html (ADR 2000, chapter 8 – Information Superiority & Space – downloaded 11 Oct 2000).
74. www.iacebter.org/bosnia/lituchy.htm (Media Deception & The Yugoslavian Civil War – downloaded 7 Feb 01).
75. www.farshore.force9.co.uk/spysat.html (IKONOS – downloaded 13 Dec 00).
76. www.jinx.sistm.unsw.edu/greenlft/1998 ('Media Deception: Practice Makes Perfect' – downloaded 7 Feb 01).
77. www.llnl.gov/csts/publications/gupta/intro.html (Commercial satellite imagery downloaded 18 Feb 01).
78. www.parliament.the-stationery-office.co.uk/pa/cm199900/cmselect/cmdt/34718.htm (House of Commons Select Committee on Defence – 14th Report – Kosovo Campaign) downloaded 28 Nov 00.
79. www.spaceimaging.com (IKONOS satellite data – downloaded 18 Feb 01).

UNPUBLISHED WORKS

80. De Nijs, A.F. '*The Impact of Deception on the Conduct of War at the Operational and Strategic Level*'. HCSC7, .March 1997.

81. Hatherley, G.C. '*Why were NATO Air Operations so ineffective against the Serbian Land Forces in Kosovo, and what Lessons can NATO learn from this?*' JSCSC, ACSC 3 Defence Research Paper, 15 Mar 2000.

82. Morris, A.J. & Others. '*The Effects of Technology on Deception*'. Australian Staff College, 1983.

83. O'Kelly D.R.E & Others. '*Consider Deception at the Operational Level to refine a set of principles for its application. Consider the implications for Deception of the technologies likely to be present in the battlefield in 2010*'. ACSC29, Group Research Paper, Camberley, 1995.

84. Pearson, G.J. '*To What Extent has the UK Intelligence Community re-organised and re-focussed to meet the security challenges of the post Cold War era?*'. ACSC3 Defence Research Paper, 2000.

85. Wray, A.D. '*Amphibious Operations & the Art of Deception*'. HCSC 8, Camberley, 1995.

NOTES

1 Whaley, B. 'Towards a General Theory of Deception and Surprise',Frank Cass,London,1982,p182.

2 Joint Doctrine Pamphlet(JDP)2/98,'Deception',MOD-CSE,p1.

3 Surprise is a Principle of War. As defined in British Defence Doctrine (JWP 0-01), 'Surprise causes confusion and paralysis and can destroy the cohesion and morale of the adversary. Deception is one element of surprise. Surprise tends to be forgotten in peace but historical analysis shows that it is a crucial pre-condition to success.'

4 Handel,M.'War,Strategy&Intelligence',Frank Cass,London,1989,p37.

5 JWP0-01,pA-5.'There must be no wasteful expenditure of effort where it cannot significantly affect the issue'.

6 Handel,*op cit*,p312.

7 BDD,p4.10.

8 UKOPSDOC,JWP0-10,PJHQ,Sep 99,p7-4

9 Britain's Small Wars:http://www.britains-smallwars.com(downloaded 14 Nov 2000).

10 Wray,A.D.'Amphibious Operations and the Art of Deception',HCSC8,Camberley,p14.

11 Handel,*op cit*,p364.

12 Soviet Military Encyclopaedia(1978): 'Complex of measures designed to mislead the enemy as to the presence and disposition of forces and military objectives; their condition, combat readiness and operations and also the commander's plans. *Maskirovka* contributes to the achievement of surprise for the actions of forces, the preservation of combat readiness and increased survivability'.

13 Dick,C.K.'Maskirovka in Yugoslav Military Thinking',Conflict Studies Research Centre,p2.

14 *idem*.

15 Kothkopf,D.J.'The Disinformation Age',Foreign Policy,No114,Spring1999,p85.

16 D/DTIO/300/1/1,MODUK,22Feb01:'The aim of OPSEC is to deny an adversary sufficient critical information that he is prevented from deducing detailed friendly intentions'.

17 Kothkopf,*op cit*,p89.

18 BDD,p2.11.

19 JWP 3-50: 'Multifunction operations involving military forces, diplomatic and humanitarian agencies in pursuit of humanitarian goals or long-term political

settlement, impartially in support of United Nations (UN) or Organisation for Security and Cooperation in Europe (OSCE) mandate'.

20 *ibid*,p6-12.

21 *ibid*,p1-2.

22 JWP3-50,p1-2.

23 Combelles-Siegel,P.'Integrating Information Activities in Peace Operations',DoD,1998,p74.

24 The 36-nation coalition failed to reach consensus on even limited psychological operations.

25 Daniel,D.C&Herbig,K,'*Strategic Military Deception*',Pergamon,p8:'The target (of deception) is the intelligence organisation of a 'state' that monitors the channels of information which may carry deceptive signals'.

26 AFM,Vol1,Part4,Part C,Ch 5,Deception,p5-1.

27 Akin to the London Controlling Section of WW2.

28 D/DTIO,*op cit*,p13.

29 Greenberg,L.T. 'Information War and International Law',NDU/CCRP,Washington,Jan1998,p-xviii.

30 JWP2/98,p1.

31 Handel,*op cit*,p361.

32 Handel,M.I.'Masters of War',Frank Cass,London,1992,p4.

33 *ibid*,p4.

34 *ibid*,p7.

35 *ibid*,p102.

36 JDP2/98,*op cit*,2/98,p1.

37 Daniel&Herbig,*op cit*,p180: Definition of Strategic Operations: the initial start of war; the opening of operations on a new front or the opening of a new attack on a dormant front.

38 D/DTIO,*op cit*,p2.

39 JDP XX-01(Draft),Mar01,p3:'Co-ordinated actions to influence an adversary in support of political and military objectives by undermining his will, cohesion and decision-making ability including his information, information-based processes and systems while protecting one's own decision-makers and decision-making process'.

40 Allied Joint Doctrine,AJP-01(A),p15-3.

41 D/DTIO,op cit,p12.

42 Tactical deception concentrates on camouflage, concealment and tactical manoeuvre.

43 AJP-01(A),*op cit*,p15-3.

44 Handel,*op cit*('War,Strat&Int'),p36.

45 JWP2/98,p3.

46 Handel,*op cit*(War,Strat&Int),p14 quotes from Mure:'Practice to Deceive'.

47 Bluheman,C. 'The Baffled Brain' 1973:quoted in Morris,A.J.,'*The Effects of Technology on Deception*',Australian Staff College, 1983.

48 Daniel&Herbig,*op cit*,p8.

49 *ibid*,p19.

50 Handel,*op cit*,('War,Strat&Int'),p37.

51 Gerwher,S.&Glenn,R.W.'The Art of Darkness–Deception and Urban Ops',RAND,2000,p29

52 *ibid*,p30.

53 Handel,*op cit*,('War, Strat & Int'),p329.

54 *ibid*,p330.

55 Poynton,D.M.'*Surprise can be achieved in war despite advances in EW & Surveillance Devices*',Australian Defence Force Journal,Nov1999,p49.

56 *idem*.

57 Dixon,N.'The Psychology of Military Incompetence',Pimlico,London,p165.

58 *ibid*,p165.

59 D/DTIO,*op cit*,p6.

60 *ibid*,p180: 'Deception had occurred if the target, even though anticipating an attack, made an error concerning either the time, nature or place of attack'.

61 Gerwher&Glenn,*op cit*,p37:quotation from Whaley,B.

62 *idem*.

63 Deception, morale, spirit, initiative, surprise and security.

64 Morris,A.J.&Others,'*The Effects of Technology on Deception*',Australian Staff College,1983,p1.

65 House of Commons Select Committee on Defence 14th Report – Kosovo,p227.

66 Handel('War, Strat & Int'),*op cit*,p340.

67 AJP-01(A),p15-2.
68 AFM Vol2,Part5,Issue2,Nov 99,piii.
69 Gerwher&Glenn,op cit,p7.
70 *ibid,* p8.
71 *ibid*,p43.
72 *ibid*,p54.
73 *ibid*,p47.
74 *ibid*,p48.
75 *ibid*,p20.
76 *ibid*, p49.
77 Poynton,*op cit* p42.
78 Dailey,B.D&Parker,P.J,'*Soviet Strategic Deception*',Lexington,Hoover Institution Press,1987,p470.
79 http://www.dtic.mil/execses/adr2000/chap8.html,p16(downloaded 11 Oct 00).
80 Space&MOD Policy, presentation to ACSC4,26 Feb 01.
81 High resolution= 'digital, pictorial representation of the Earth's surface where the length and width of each pixel represents a ground distance of 4m or less'.
82 www.llnl.gov/csts/publications/gupta/intor.html(downloaded 20 Oct 00),p1.
83 http://www.llnl.gov/csts/publications/gupta/buyers.html(downloaded 13 Dec 00),p1.
84 http://www.spaceimaging.com(downloaded 18 Feb 01).
85 http://imagesatintl.com(downloaded 26 Feb 01).
86 http://www.eorc.nasda.go.jp/ALOS/set(downloaded 18 Feb 01).
87 http://www.fas.org/spp/guide/europe/military/weu/1643e.htm(downloaded 21 Mar 01).
88 *idem*.
89 http://www.llnl.gov/csts/publications/gupta/observations.html(downloaded 13 Dec 00),p1.
90 Around 40 spacecraft are capable of imagery of 10-1m GSD
91 http://www.llnl.gov/csts/publications/gupta/buyers.html(downloaded 13 Dec 00),p2.
92 http://www.fas.org/spp/military/docops/operate/ds/images.htm (Desert Storm-Military Space Intelligence, downloaded 22 Mar 01).
93 *idem.*
94 *idem*.
95 Presentation on US Space Policy by US Space Command to ACSC 4,26 Feb 01.
96 Space & MOD Policy, presentation to ACSC4,26 Feb 01.
97 http://www.fas.org/spp/military/program/imint/lacrosse.htm(downloaded 17 Feb 01). The LACROSSE satellite has a solar array wingspan of 50m
98 Space & MOD Policy, presentation to ACSC4,26 Feb 01.
99 The German/UK 'Terra SAR' programme envisages the launch of a 1.5m resolution SAR sensor in 2004.
100 www.fas.org/irp/program/collect/jstars.htm(downloaded 17 Feb 01 (last updated 25 Jul 99)).
101 http://www.dtic.mil/execses/adr2000/chap8.html(downloaded 11 Oct 00),p16.
102 Mason,T.'*The Aerospace Revolution*', Brassey's,London,1998,p94.
103 www.fas.org/irp/program/collect/jstars.htm(downloaded 17 Feb 01 (last updated 5 Mar 00)).
104 Mason,*op cit*,p4.
105 Davis,M.*The RMA in Asia-The Stillborn Revolution?*',RUSI,London,2000,p265.
106 Mason,*op cit*,p4.
107 Sanders, D.'*Russia's Security Challenges*' *in International Security in a Global Age*' (Eds Jones,C and Kennedy-Pipe, C),Frank Cass,London,2000,p67.
108 Mason,*op cit*,p35.
109 *ibid*,p37.
110 Janes's Radar & EW Systems,11th Ed 1999-2000,p203.
111 http://www.fas.org/nuke/guide/russia/airdef/a-50.htm(downloaded 21 Mar 01).
112 Jane's,*op cit*,p201.
113 D/DTIO,*op cit*,p3.

114 ACSC4,Annex B to Serial 2:Media Ops,p6.
115 *idem*.
116 *ibid*,p23.
117 *ibid*,p22.
118 Duncan,A.'*Mixing with the Media*',British Army Review,Aug,1995,p17.
119 Float,R.A.'*Armed Forces & the Media:Improving the Relationship*',British Army Review,No125,2000,p85.
120 *ibid*,p86.
121 Duncan,op cit,p23.
122 Carruthers,S.L.*The Media at War*',p124.
123 *ibid*,p133.
124 *ibid*,p138.
125 Duncan,*op cit*,p21.
126 Carruthers,*op cit*,p160.
127 Mueller,J.'*The Perfect Enemy:Assessing the Gulf War*',Security Studies No1,Autumn,1995,p99.
128 Bayldon,R.'*Op GRANBY-Deception in 1 Armd Div*',DSc(Land) Note12/92,Jun92,p17.
129 Mueller,*op cit*,p98.
130 Carruthers,*op cit*,p137.
131 ACSC4 Media Ops,*op cit*,p25.
132 *ibid*,p45.
133 Handel('War, Strat & Int'),*op cit*,p417.
134 Whaley,*op cit*,p179.
135 Daniel&Herbig,*op cit*,p5.
136 Hatherley,G.C.'*Why were NATO Air Ops so ineffective against the Serbian Land Forces in Kosovo?*',JSCSC,ACSC3,2000,p8.
137 *ibid*,p18.
138 *ibid*,p5.
139 Poynton,*op cit*,p49.
140 Handle,M.I.'*Perception,Deception and Surprise:the case of the Yom Kippur War*',The Hebrew University,Jerusalem,1976,p17.
141 *ibid*,p14.
142 *idem*.
143 *ibid*,p24.
144 *ibid*,p14(quoting Whaley,B).
145 Dailey&Parker,*op cit*,p478.
146 AJP-01(A),p15-3.
147 http://www.fas.org/spp/military/docops/operate/ds/images.htm(Desert Storm-Military Space Imagery Intelligence,downloaded 22 Mar 01).
148 http://www.fas.org/spp/military/docops/operate/ds/images.htm(Desert Storm-Military Space Imagery Intelligence,downloaded 22 Mar 01).
149 Poynton,*op cit*,p46.
150 '*Concealment&Deception by Modern Camouflage Techniques*',Armada International,1986,p90.
151 O'Kelly,D.R.E&Others,'*Consider Deception at the Operational Level to refine a set of principles for its application*.',ACSC29,1995,p10.
152 AFM,Vol1,Part 4,Part C,Ch5,Deception,p5-2.
153 Cobbold, R.'ASR2 – An Acronym for the Millennium', p3.
154 Morris,*op cit*,p23.
155 O'Kelly,*op cit*,p8.
156 www.mitre.org/technology/imagery_systems/jsips.html,17 Feb 01.
157 Wray,*op cit*,p12.
158 Western media believed themselves to have been used to support the deception plan because attention was concentrated on amphibious training.
159 Gerwher&Glenn,*op cit*,p49.
160 Tactical level deception may suffer as action occurs in real-time or near real-time.
161 AJP-01(A),*op cit*,p15.
162 Glantz,D.M.'Surprise and Maskirovka in Contemporary War',Military Review,Dec88,p51.(Kir'yan emphasises *maskirovka* at all levels against technological reconnaissance').