AIR POWER STUDIES CENTRE

PAPER 47

Month Year

MILITARY INFORMATION OPERATIONS IN A CONVENTIONAL WARFARE ENVIRONMENT

By

C.J. Westwood

About the Author

The ...

INTRODUCTION

> You bring me 10 hackers and within 90 days I'll bring this country [USA] to its knees.[1]

Envisaging how information-based technology will influence the way societies will function beyond the next decade has become extremely difficult. This is a result of the increasing pace of development of Information Technology (IT) and the dramatic increase in the diversity of applications in which IT systems are now being employed. Evidence indicates that many nations throughout the world are becoming dependent on their technology-based information systems to generate national wealth and, amongst other things, to develop and employ military capabilities. As a result of this dependence, national power in the future will be increasingly influenced by the capabilities of the national information infrastructure.[2]

Postulating beyond such a broad vision of the influence of technology into the next century, while interesting, is of little direct relevance to most of today's society. This is not the case, however, for those tasked with ensuring national security. Because armed force is likely to remain a key element in national security, military planners must prepare for the onset of the information age, and in particular they must consider the ramifications of information technology and information power for future national security.

As the advanced nations become more dependent on their information resources, a new vulnerability has emerged. The potential for serious damage to be inflicted upon a nation by an attack on its national information infrastructure is now a reality. US analysts estimate that there were approximately 250,000 attacks against the US Defense Department information systems in 1995.[3] This new threat has given rise to the concept of Information Warfare (IW). Although initially IW was considered as pertaining primarily to military information operations in support of conventional warfare objectives, the world's security analysts are now beginning to seriously consider the emergence of an IW as a new paradigm of warfare. This emerging paradigm establishes IW conceptually at the same level as 'Conventional Warfare', and challenges security planners to re-think the established strategies, doctrines and cultures that have existed within industrial age military forces for over 100 years. If the IW paradigm fully matures, some future conflicts may conceivably be fought exclusively in the information domain. In such a conflict the objective would be the control of all or part of another nation's information infrastructure, and hence potentially most of their wealth generating mechanisms.

[1] Mr Jim Settle, the former head of the FBI's computer security section, as reported in *The Australian*, 18 June 1996, p 59.
[2] An information infrastructure includes both information systems and an intellectual base on which to further develop information systems.
[3] Cooper, P., US Lawmakers Examine Vulnerabilities of Internet, *Defense News*, 27 May - 2 June, 1996, p 37, attributed to Senator Sam Nunn.

The consideration of doctrinal, cultural and technical strategies that will prepare a nation for conflict in such a future environment is therefore essential.[4] But, it is the information tools and techniques which are commonly available today, and which may be used as weapons against existing conventional military capabilities, that are of more immediate concern. When used in a military environment, the combination of these tools and techniques have been termed Military Information Operations (MIO). This paper will introduce the concept of MIOs and will describe the specific elements of the MIO environment that can be used to develop information strategies for supporting conventional warfare objectives. It will also espouse a series of principles that should guide the development of an MIO capability. Finally, the paper will discuss the relationship between information operations and other more traditional elements of the conventional warfare model.

INFORMATION OPERATIONS IN A CONFLICT ENVIRONMENT

The ability to generate and assess information in a timely manner has long been regarded by military decision makers as vital. Information gathering and processing tools have evolved dramatically in line with recent technological developments. This has increased the importance of information within military forces to the extent that technology- based information systems are now a significant (some would argue decisive) component of the conventional warfare inventory. Technologies are currently being developed in the commercial environment which will elevate the role of the information system beyond that of collecting and processing information. Information systems may now be applied by military forces as both offensive and defensive weapons. This has prompted many to proclaim the arrival of the era of the information war.

The 1991 Gulf War is often cited as the first information war. During the Gulf War, the Coalition forces targeted the Iraqi information environment with an array of high-tech weapons including precision guided munitions, first generation information and computer weapons, and a number of intelligence, surveillance and reconnaissance sensors. These were employed with devastating effect, initially to disable the Iraqi air defence system and then to isolate the Iraqi leaders from their deployed forces by targeting the Command and Control (C^2) system. The operations against the Iraqi information environment significantly contributed to Iraq's ultimate demise. Throughout the war, however, aircraft still dropped bombs in Iraq and Kuwait on non-information targets, and Coalition ground troops were deployed to expel Iraqi forces from Kuwait. This was not the first information war.[5] Rather, the Gulf War was the

[4] The paradigm of IW is discussed at length in *'The Future is Not What it Used to Be: A guide to conflict in the information age'*, scheduled for publication by the Air Power Studies Centre in late 1996.

[5] The most widely read book that claims that the Gulf War was an information war was written by Alan Campen, *The First Information War*, AFCEA International Press, Virginia, 1992. This book is an excellent document which presents an overview of the information aspects of the Gulf War. However, I do not agree with the conclusion drawn from the book that the Gulf War was indeed the first information war. Conventional war objectives, not information objectives, lay at the heart of the Gulf campaigns. The Gulf War simply demonstrated the rapid advances in technology that had been made since the US had previously undertaken a war of this scale.

most graphic example of the use of information operations to support conventional warfare objectives that the world has witnessed to date. The Gulf War clearly pronounced to all military planners that MIOs are likely to be used in the future for achieving conventional warfare objectives, and therefore should be included in any future military inventory.

The specific tools and techniques that comprise MIOs, as well as the principles that govern their development and employment, must be understood by those charged with integrating information operations into existing conventional military forces. While Figure 1 highlights some of the individual elements of the information operations environment, these are by no means definitive. Figure 1 is neither intended to represent every possible component of the information operations environment, nor designed to suggest that the individual elements that comprise information operations can be neatly divided into discrete boxes.

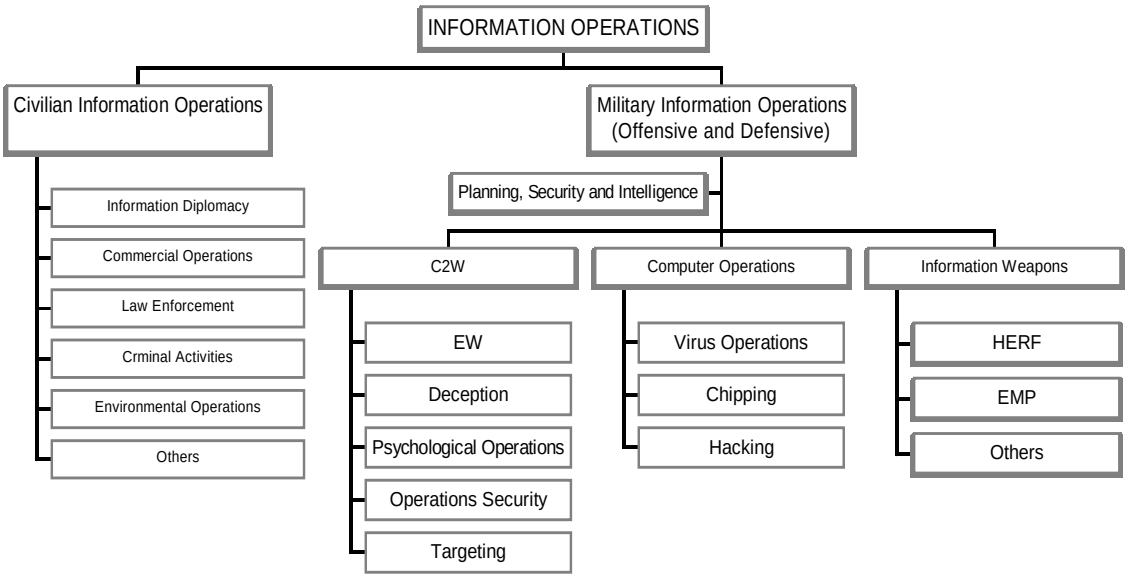

Figure 1 - Information Operations Schematic Diagram

The information operations environment is complex and multi-dimensional, consisting of many interrelated and often interdependent activities. These activities will often occur simultaneously, and in support of strategic, operational and tactical objectives. Skills required to accomplish the information operations activities must be drawn from a variety of existing disciplines, leading in time to the development of a specialist information warrior profession. The activities are ultimately intertwined to create a series of complex information strategies. Figure 1 simply highlights the essential elements that must be considered within an overall information framework. The representation also presents a checklist of activities that nations or organisations may wish to consider as they increase their dependence on IT.

The individual elements of Figure 1 will now be discussed, with particular emphasis on the military applications of information operations. However, distinguishing between military and civilian information responsibilities is not a simple task, and requires consideration of several complex issues.

CIVILIAN/MILITARY INFORMATION OPERATIONS

National information infrastructures are becoming an important vehicle for the generation of national wealth throughout the developed world. National information systems are, amongst other things, already used to conduct commerce and regulate and control national production. Nations are becoming increasingly dependent on their information infrastructure as the information age evolves. Accordingly, this infrastructure may now be considered as representing an extension of national sovereignty and any attacks on national information systems may be perceived as attacks on the nation itself.

A further argument may be that the national security implications of information attacks make the defence against such attacks a military task. If this is the case, the vast majority of the world's military forces require a significant review of their current doctrine and capabilities. Most are presently not capable of operating in a hostile information environment. An alternative argument may be that attacks against national information systems are criminal in nature and are therefore the responsibility of national police forces. Again, most police forces are incapable of defending against such attacks. Indeed, there is probably no organisation in the world that can adequately defend national information infrastructures as yet. Regardless of the capabilities of the various organisations, a clear observation is that the jurisdiction boundaries that separate civil and military security responsibilities are blurring as the information age evolves.

Separating military and civilian information operations, particularly as they pertain to defending national information systems, is also complicated by the military dependence on the civilian information infrastructure. Significant elements of many of the information systems used by the world's modern military forces are designed, developed and managed by civilians, primarily for civilian purposes, and make extensive use of the civilian information infrastructure. This is particularly the case with communication systems. The use of unique systems by the military forces for all of their information tasks is not economically viable. Therefore, an attack that targets a military capability via a multi-user information system may inadvertently disrupt civilian users. Likewise, an attack which is directed at a civilian user of an information system may inadvertently affect military users. Is a military or civilian response more appropriate in each of these cases? To many this may appear to be a trivial issue, but distinguishing between civilian and military information operations is important if an appropriate (and legal) national response is to be determined.

The identification of the source of an information attack can be difficult, at times impossible, and can contribute to the problem of determining an appropriate response. Following a skilled information attack, identifying whether the act was calculated and hostile, or simply an accident or a system error may well be impossible. Determining whether the attack was committed by a nation, or an individual or non-nation state organisation may also be impossible, as may be ascertaining the extent of any damage caused. Given the embryonic state of international law pertaining to the information domain, pursuing a response through the courts may also be impossible and/or pointless. Therefore, while distinguishing between an MIO and a Civilian Information Operation (CIO) is highly desirable, and from a legal viewpoint it may be essential, such distinction is often impossible.

Attempting to resolve tomorrow's information security challenges with today's security infrastructure and culture is unlikely to prove successful. Securing a national information infrastructure presents unique challenges to national security agencies and demands unique and innovative solutions.

The need for macro-level information security in the information domain is becoming more obvious. There is a strong argument for the development of a national information authority which has the responsibility for assuring the integrity of all national information systems, advising on the development of new information systems, sponsoring research and development into information-assurance technologies, and ultimately prosecuting information operations in support of diplomatic, counter-criminal and conflict resolution objectives.

A national information authority would offer many strategic opportunities and benefits (including significant efficiencies) and could comfortably address information issues across portfolios, including national security and defence considerations. Such an organisation would not deny the individual elements of a nation's armed forces the right to develop their own information strategies; indeed, all arms have both a single-service and joint responsibility to develop robust information strategies now. The further a nation travels down the information age path, however, the more necessary the development of a professional, specialist national information body appears. It is an option that should be considered by any government with a genuine commitment to national security.

MILITARY INFORMATION OPERATIONS

The previous discussion addressed the difficult delineation between military and civilian information operations. The following discussion highlights what actually constitutes an MIO by examining each of the three terms.

Military

A look into the future warfare environment indicates an increasing role for information operations and the emergence of IW as a new paradigm of warfare. Military planners must therefore prepare to develop information skills and strategies as part of their immediate capabilities and, ultimately, they must prepare their force for involvement in full scale information wars. These planners must also remember that IW is emerging as a paradigm of *warfare*, not a paradigm of information. Regardless of the extent that the IW paradigm influences the future warfare environment, war will still be war, and thus will still involve the human factors that have been associated with conflict since the dawn of time. While there may be less blood shed in an information war, human suffering will, in all likelihood, result. The legal and diplomatic consequences of war will also remain much the same. Information technology does not make war any more acceptable to a civilised society. Therefore, while the information systems, tools, techniques and strategies of the military and civilian information warriors may be common, and indeed complementary, a nation as a whole, and the military profession in particular, must not forget the significance of the M in MIO.

Information

Although seemingly self-explanatory, understanding the nature of information is important. Information is the product of the processing of data, while data is simply the product of some observation. The processing of data into information involves placing the data into some form of context. This context can be the formation of a sentence or other human readable form, a machine readable sequence, or the classification of the data against some known measurement, such as time, height, weight, etc. The result is information and this is created and manipulated to enable decisions to be made. Although most decisions are made by a human, increasingly decisions are being made by rules-based or knowledge-based systems, and, although currently limited in application, some artificial intelligence systems.

Information, or any developed form of the information, is only one part of an information system. An information system consists of data (both as an initial input and as stored in various parts of the information systems in the form of information), hardware, software, communications, people and procedures. Any one of the individual elements of the information system, as well as the information system processes which convert the raw data into various forms of information, may provide a suitable target on which influence may be exerted. The information system as a whole, therefore, is the target of information operations, and not just the information itself or its associated technology.

Operations

Information operations seek to influence the decision making process. MIOs are not information technology support activities, such as system management and system administration. They are activities directly focussed on warfare and include offensive and defensive activities aimed at all levels of the decision making process. In the modern warfare environment, attacking and defending information systems is a vital combat task, and strategies must be considered in conjunction with the wider military plan. When correctly applied, offensive information operations can be just as lethal as the employment of conventional weapons. As an example, certain aircraft flight control systems may be shut down using MIO techniques. The resultant crash will destroy the aircraft, and generally kill the pilot and crew, just as effectively as the best air-to-air missile.

An MIO, therefore, is:

> Any activity that consciously targets or protects the elements of an Information System in pursuit of military objectives.

PLANNING, SECURITY, AND INTELLIGENCE

The planning, security and intelligence considerations of MIOs must be present in all aspects of the MIO development process. These issues are fundamental to the success of MIOs.

Planning

Information operations, like most operations, can only be effective when adequate attention is given to the overall objective to which they are being applied. Developing an MIO strategy requires careful adherence to planning philosophies, starting with the development of an achievable aim. The main objective of planning is to assure that information operations within the MIO environment are focussed on the wider military strategies and therefore the security objectives of the nation. This requires the development of formalised planning procedures.

Security

Military operations are most effective when they surprise an enemy. Surprise can only be achieved when security procedures deny enemy access to friendly intentions, strategies and capabilities. This applies to the MIO environment as much as it does to any other discipline of warfare. Security is therefore an issue that must be considered throughout an MIO program. The integrity of friendly software, hardware, communications, procedures, people and strategies is an essential part of the MIO environment. Developing a detailed strategy for information operations is pointless if that plan is known to enemy forces.

Security measures for information systems must not be reliant on one particular aspect of that system. For instance, many new systems are being created with in-built software security systems. These systems will alert users if infiltration into the system is suspected. While these systems might be useful in highlighting the amateur infiltrator, skilful warriors may either attack the warning software before attacking the main software, or conversely they may attack the system via an alternative element, such as the hardware. Therefore, information security must address each of the elements of the information system, including the people. Getting routine procedures right, and addressing the cultural issues associated with security, will often reap greater benefits than using the most elaborate software or hardware protection devices. Information security is a significant activity in the MIO process. Unless this activity is successfully accomplished, the rest of the MIO effort may well be doomed to failure.

Intelligence

Intelligence provides IW practitioners with assessments of an enemy's information systems and their likely reactions, both human and machine directed, following the commencement of an information attack. Information systems are dynamic in nature and their configuration can be changed with minimal effort. Planning attacks against such systems therefore requires refinement in response to such changes, often at the last minute and occasionally during an attack. Accordingly, employment of successful MIO strategies demands comprehensive and real-time intelligence support.

COMMAND AND CONTROL WARFARE

Of all the activities that have emerged with the evolution of IW and information operations, Command and Control Warfare (C^2W) has attracted the most attention.

Lieutenant Colonel Norman Hutcherson (United States Air Force), provides an excellent overview of C^2W in his paper *Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base.* But simply providing a synopsis of that document, although tempting, must be avoided when considering C^2W from an Australian perspective. The American approach to C^2W is comprehensive. They have committed substantial resources to the development of technologies, doctrine, strategies and organisations that will equip them to meet an information threat in any future conventional war. Australia, however, like most non-superpower nations of the world, will not be able to commit the substantial resources needed to follow the American model. Therefore, while much of the descriptive overview of C^2W is taken from Lieutenant Colonel Hutcherson's works, the general approach taken in this paper is tempered by the economic realities which will dictate the degree to which mid-level powers can invest in their own strategies.

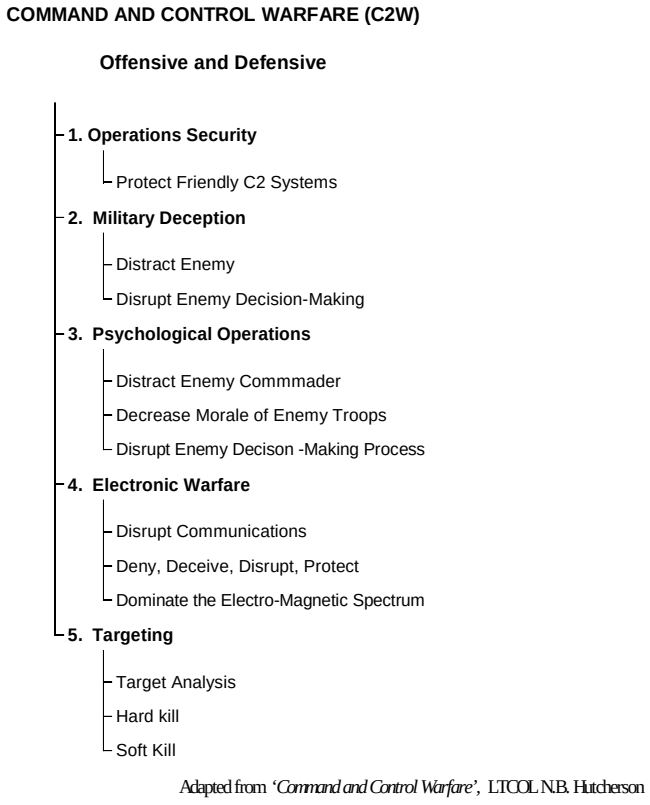

Figure 2 - The Five Pillars of Command and Control Warfare

Command and Control Warfare (C^2W) is:

> the approach to military operations which employs all measures (including but not limited to Electronic Warfare (EW), military deception, psychological operations (PSYOPS), operations security and targeting), in a deliberate and integrated manner, mutually supported by intelligence and information systems, to disrupt or inhibit an adversary's ability to command and control his forces while protecting and enhancing our own.[6]

[6] HQADF Study Team Report, *Command and Control Warfare,* November 1995, para 5.16.

C^2W is the war-fighting or tactical application of MIOs and is usually aimed at a specific and defined battlespace, although it may be conducted in conjunction with other MIOs which may be focussed on strategic information targets. There are five individual elements of C^2W, covering both offensive and defensive applications. These are illustrated at Figure 2.

Operations Security. Operations Security (OPSEC) is a term that appears in many military documents in almost as many contexts, with several apparently different meanings. OPSEC is a process used for denying adversaries information about friendly disposition, intentions, capabilities, or limitations.[7] It requires the employment of specialist equipment, including software, the adoption of suitable procedures, and importantly, the development of a pro-security organisational culture. OPSEC is equally important as a defensive posture as it is in developing offensive strategies. By denying a potential enemy an understanding of the capabilities of friendly systems, possible hostile C2W will be more likely to miscalculate the friendly information capabilities and be ineffective.

Military Deception. Military deception is used to inject ambiguity and create false assessments in the decision-making process of the enemy. The objectives of employing military deception are to create a false deduction of friendly intentions, capabilities and/or dispositions, by the enemy. The target of deception is the enemy decision-maker, that is, the individual who has the necessary authority to make a decision. There is no point influencing a decision if, in the event of ambiguity, the decision-maker passes the decision to a higher authority. In this case, the higher authority must also be the target of deception.

Psychological Operations. Psychological Operations (PSYOPS) are operations which are planned activities in peace and war directed to enemy, friendly and neutral audiences in order to influence attitudes and behaviour affecting the achievement of political and military objectives. The objective of PSYOPS is to cause enemy, friendly and neutral personnel to act favourably toward friendly organisations.[8] PSYOPS have been used throughout history to influence adversary leaders and groups. The expansion and development of information technology, and associated global media coverage, has enhanced modern PSYOPS opportunities.

Electronic Warfare. Electronic Warfare (EW) is the military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum.[9]

Targeting. Targeting is not just a process, nor is it just focussed on destructive ends. 'Targeting is a capability'[10] that emphasises the requirement to collect, process and interpret information regarding decisive points in an enemy's command and control system, and then selects the most effective option of incapacitating them. There are

[7] US Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms,* December 1989, p. 265.
[8] Australian Defence Force Publication - 25, Psychological Operations, para 101.
[9] Australian Defence Force Publication - 24, Electronic Warfare, para 105.
[10] HQADF Study Team Report, *ibid*, paras 5.18-5.20.

many hard and soft kill options available to a commander. Soft kill options include the use of EW, strategic computer operations and information weapons, while hard kill options refer to the various means of physically destroying targets.

Hard or soft destruction requires the capability to remove selected targets from an enemy's order of battle. These targets include vital communication nodes, national infrastructure, vital personnel and specific military equipment. Destruction may be achieved by any arm of the military. Physical destruction has the highest risk associated with its application and, unlike the other elements of C^2W, physical destruction tends to be permanent, that is, buildings are destroyed and people are killed. This can be either a desirable or undesirable outcome, and so must be considered when strategies are being developed. The diplomatic recovery time for physical destruction is usually considerably longer than that of the other elements. Accordingly, even though it is often the most effective method of demonstrating resolve, physical destruction is generally used as a last resort. However, a commander must have the option of employing hard and soft kill options to accomplish a desired C^2W effect.

The Objective of C^2W

Until the 1991 Gulf War, the C^2W elements had rarely been used in conjunction with each other to specifically target an enemy's ability to command and control its forces. In the Gulf War post-mortem the advantages of combining the five elements in pursuit of a single objective were realised and true C^2W born.

The ultimate objective of C^2W is to 'decapitate the enemy's command structure from its body of combat forces,'[11] while ensuring the integrity of friendly command and control systems. C^2W aims to reduce the uncertainty of combat by creating a battlespace that becomes more predictable for friendly forces as the C^2W effort increases, while becoming exponentially less predictable for the enemy. C^2W activities seek to lift the fog of war for friendly forces while thickening the fog for the enemy. C^2W strategies focus the five elements specifically on the decision cycles of both friendly and enemy forces. Therefore, the aim of C^2W is to gain, maintain, or widen a gap in the effectiveness of C^2 in favour of friendly forces throughout a campaign and particularly at decisive points in a battle.

C^2W and the OODA Loop

The often quoted OODA (Observation, Orientation, Decision, Action) loop has been adopted as the focal point of C^2W. The concept of the OODA loop had its origins in the Korean war where an American pilot, John Boyd, identified the advantages of having good visibility and sensitive controls on board the US Sabre jet fighters. Although the Russian MiG 15s were faster, more powerful, more manoeuvrable, and could sustain greater bank angles, the American jets were consistently victorious in air to air engagements. Boyd explained that the US pilots simply had a shorter total period between observing an event, orientating themselves to the possible ramifications of the event, making a decision and acting. The value of a relatively short decision cycle was realised. Since the inception of air to air combat, staying

[11] CJCS MOP 30, *Command and Control Warfare,* 1st revision, 8 March 1993, enclosure 3.

inside the enemy's decision loop has been a consistent objective. Since Boyd's analysis, this has been a recognised objective of many forms of warfare.

The OODA loop concept is now applied to most aspects of modern warfare, from land manoeuvres to strategic missile developments. The OODA loop can also be seen to operate in the business world. Those who are quick to observe an opportunity, recognise it and exploit it are more frequently the successful or victorious business persons. The OODA loop theories can be found in the heart of modern C^2 systems and consequently in modern C ^{2}W strategies. Successful C ^{2}W operations will therefore increase the enemy's decision cycle - his OODA loop - to such a point that he will become increasingly vulnerable to attack.

C ^{2}W in the Gulf War

In the 1991 Gulf War, the Coalition forces attacked the Iraqi C^2 system from the outset. Even before the war had commenced, EW, PSYOPS, and deception were employed for influencing the Iraqi people and hierarchy. During the first hours of the air attacks in Iraq, information systems and communication devices were targeted, and in many cases physically destroyed, leaving the huge force that had occupied Kuwait completely cut off from the commanders in Baghdad. The Iraqi air defence system was virtually shut down by Coalition activity within hours of the commencement of *Operation Desert Storm*. The extant Iraqi air defence system was amongst the most extensive in the world. Shutting such an extensive system down with apparent ease was a significant achievement and the result of a calculated offensive involving all of the C ^{2}W elements. This early success gave the Coalition forces air supremacy. In turn, this supremacy significantly reduced the potential for Coalition air fatalities and allowed the Coalition air forces to strike Iraqi ground targets almost at will. The Coalition forces effectively destroyed the ability of the Iraqi military commanders to observe, and the Iraqi OODA loop was significantly increased.

In conventional wars that may follow the Gulf War, defence of friendly C^2 systems and attacks on enemy systems will be of paramount importance.[12] The side with the smallest decision cycle will have a decided and, probably, decisive advantage. As Sun Tzu observed:

> A confused army leads to another's victory.[13]

COMPUTER OPERATIONS[14]

One of the more recent additions to the military commander's toolbox is the computer. Computers, and associated technology have helped change the face of modern warfare by providing the capabilities to generate and process massive amounts of data, and disseminate the resultant information throughout the battlespace.

[12] For further discussion see, Campen, A.D., *The First Information War*, p xi.
[13] Griffith, S.B., *Sun Tzu: The Art of War,* Oxford University Press, London, 1963, p 82. Emphasis added.
[14] This section has been drawn extensively from Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, Thunder's Mouth Express, New York, 1994, Chaps 9-11, and Daniel E. Magsig, *Information Warfare in the Information Age,* extracted from the Internet.

However, computers provide more than just an information processing capability. They may also be used as weapons in their own right. The most common examples of computer operations include hacking, virus planting and chipping. These techniques are primarily aimed at targeting the enemy's broad information environment. However, they may also be used to attack the enemy's computer-based weapon systems and computer-based platforms, such as 'fly-by-wire' aircraft. Although generally strategic in nature, computer operations may be applied to the tactical and operational components of the conventional warfare environment, either in support of C^2W operations or in direct support of air, land or sea operations.

Hacking

The term computer hacker is now synonymous with computer criminal although, arguably, this merging of terms is not justified. Someone who uses a computer to rob a bank is a criminal, not a hacker. The genuine computer hackers are still doing what the original computer hackers were doing 40 years ago - simply exploring the bounds of computer science.

Unfortunately, exploring today's computer science often means entering other people's systems. There are many computer hackers around the world who enter other people's systems on a daily basis. Most simply gain access to the systems, 'snoop'[15] around for a while, and leave. Some hackers like to explore the logic flow in systems. A few like to exploit these systems for either their own gain or simply to make life difficult for the users of that system. The genuine hackers, while invading system privacy, rarely damage the systems into which they have hacked. However, most users of systems understandably find it an unacceptable invasion of their privacy to have people intruding into their systems.

Hackers present a genuine problem to most organisations today, and a specific threat to military security. Hackers have historically found the challenge of breaking into so called 'secure' military systems one of the more satisfying aspects of their hobby. Accordingly, the first and foremost aim of any information strategy for military forces must be to defend their own system integrity.

Once access is gained into a system, hackers can generally manipulate whatever files they wish. They will often set up personal accounts for themselves in case they wish to return again in the future. A hacker can of course collect very important information. In the business domain, intelligence can be gained about a competitor's product. In the government service domain, sensitive personal information can be obtained (or altered) which can later be used against individuals. In the military domain, classified information such as capabilities, vulnerability, strategies and dispositions may be extracted or manipulated. A hacker can also change the file structure, amend the logic flow, and even destroy parts of the system.

Hacking is no longer simply a pursuit of misfits and computer scientists; it is now a genuine method of obtaining information by government agencies, criminals or subversive organisations. There have been several reports about government

[15] The term 'snoop' refers to the activities undertaken by hackers once they have entered a system.

sponsorship of such activity. Phillip Knightly reported recently[16] that many of the world's secret security organisations are now passing industrial secrets to their nation's domestic businesses. The basic tool kit of today's industrial spy contains a PC and a modem. The industrial spy is simply a hacker who intrudes into someone else's computer system and then exploits the information obtained. Neither domestic nor international laws adequately address all of the issues surrounding hacking. Therefore, in the unlikely event that hackers are caught,[17] in many situations prosecution is impossible.

The impact on those involved in developing MIOs is that hacking presents a genuine threat to the security and integrity of both military and civilian information systems. Defence against hacking can be successful to varying degrees. Most defensive strategies are system-dependent; therefore, listing them in this paper would be pointless. However, defence against hacking needs to be considered by anyone who manages or operates an information system.

The other reason that national security forces should become involved in hacking is the potential benefits that can be derived by employing hacking techniques as an offensive tactic. Intelligence collection against information stored in an enemy's databases as well as the specific system capabilities, vulnerability and architecture can be accomplished successfully using hacking techniques. In future wars, information derived from hacking will form a large part of intelligence databases and thus manipulation of the enemy's decision making support systems will become routine.

Viruses

A virus is a 'code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces'.[18] Protecting against computer viruses has become a part of using modern information systems. Viruses are passed from computer to computer via disks and reportedly via the more recent practice of electronic file transfer, such as email. Although statistics concerning viruses are often difficult to substantiate, some specialists estimate that there are as many as 3,500 viruses currently existing on the Internet, with cures being available for only 750.[19] While virus screening software should prevent known viruses being brought into a system, they will not prevent all virus attacks. The most effective method of minimising the risk of virus attack, and minimising the damage caused by viruses in the event of an attack, is by employing sound and rigorous information management procedures.

[16] Knightly, P., 'Espionage: Business as Usual', *The Weekend Australian*, 11 May 1996, p 31.
[17] Although it is difficult to determine exactly how many hackers are actually caught, various papers have suggested that about five per cent of system infiltrations are detected, and of these about 20 per cent prompt any action (mostly internal). In Australia, there are few records published; therefore these estimates are deduced from American and European figures (it obviously doesn't happen here in Australia!!)
[18] Russel, D., and Gangemi, G.T., *Computer Security Basics*, O'Reilly and Associates, 1994.
[19] Many of these viruses are derivatives of other viruses, therefore cures for one virus may be effective for a 'family' of viruses. Estimating how many 'families' of viruses are currently available is very difficult. Industry specialists interviewed as part of the research for this paper suggest that there are 300-500 'families' currently available.

Isolating Internet systems from operating systems where practical is vital. Minimising computer to disk to computer transfers, particularly if the origin of that data is the Internet, will reduce the chances of picking up a virus. The use of the most recent anti-virus software and the screening of disks every time that they are placed in a computer will reduce the risk of disk infections being passed onto systems. Careful selection and management of passwords may deter a potential intruder from accessing a system and planting a virus, while the maintenance of comprehensive system backups can minimise the impact of viruses should one find its way onto a system. Viruses, however, can also be backed up and a dormant virus can infest any backup files and can be re-introduced when a system is recovered. Accordingly, a layered backup strategy is imperative.

Anti-virus strategies are aimed at minimising the chances of getting a virus and minimising the damage that viruses can cause if they are introduced. Users of today's information systems must be aware of the virus threat. Simple procedures will often be enough to avoid viruses but a single failure to comply with anti-virus procedures can result in systems becoming inoperable.

Virus planting is clearly a suitable and attractive weapon for military forces and is a valuable addition to the offensive information operations inventory. If a simple virus can be injected into the systems of a potential enemy, the need to expend effort in physically attacking that system may be eliminated.

Chipping

Most people are aware of the vulnerability of software to hostile invasions, such as a virus attack. Few, however, are aware of the risk to the essential hardware components of an information system. Chipping is a term which refers to unexpected events that can be engineered into computer chips. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they can initiate unexpected events at a specific time, or at the occurrence of specific circumstances. This may explain why some electronic goods fail a short time after the warranty has expired. There is almost no way of detecting whether a chip contained within a piece of equipment has been corrupted.

One way to minimise the risk of chipping is to self-manufacture all important chips, such as those which are used as part of an aircraft's flight control system. Economically, this is often not feasible. Most chips used within today's high technology equipment are manufactured in countries where labour costs are low. Establishing an indigenous manufacturing capability would increase the cost of acquiring the equipment. A risk assessment must be made when purchasing vital equipment from overseas, by comparing the risk of vital equipment failing once hostilities commence to the cost of producing chips internally or developing rigorous quality control of imported chips.

Chipping represents a simple way to develop a conventional military advantage by those countries that regularly export military equipment. In the event of any hostilities with recipients of their 'chipped' equipment, that equipment may be incapacitated without having to use conventional force. This makes economic as well as military sense. The legal and ethical aspects are a separate issue.

Summary of Computer Operations

There are many other computer weapons that can be used in conjunction with or instead of chipping, viruses and hacking. These weapons have many different descriptive names such as 'worms', 'trojan horses' and 'logic bombs' and are commonplace in today's information society. They are all examples of computer operations which may be adapted to suit the warfare environment. A detailed description of all of these techniques is beyond the scope of this paper. Suffice to say that computer weapons should be an integral part of any information operations strategy. They should be considered as valid alternatives to conventional weapons both in offence and defence.

INFORMATION WEAPONS

There are several weapons currently available that can negate, destroy or incapacitate information systems, with many more being rapidly developed. Within this paper these are broadly grouped into three main types: High Energy Radio Frequency (HERF) guns, Electro-Magnetic Pulse (EMP), and other information weapons.

HERF Guns

A HERF Gun is a device that directs high power radio energy at an electronic target. Electronic circuits are vulnerable to overload; a HERF Gun simply overloads particular circuits to disable specific pieces of equipment that are dependent on that circuit. A HERF Gun can be designed to cause varying degrees of damage from simply shutting a system down to physically destroying equipment. Pointed at a computer, a HERF Gun may either permanently or temporarily terminate its operations; a HERF Gun pointed at a 'fly-by-wire' aircraft may trigger a catastrophic failure.

Although currently limited in range and destructive capacity, in the near future HERF Guns are likely to be substantially more capable and freely available and therefore must be taken seriously. HERF Guns represent an excellent addition to the offensive military inventory of a nation, and also a significant threat if possessed by an enemy. The defensive measures that can be employed to reduce the risks of HERF attacks are not well developed at this stage, but include using Gaussian shielding, gaseous discharge devices and the maintenance of physical separation.

Electro-Magnetic Pulse

Electro-Magnetic Pulse (EMP) has been described as 'the next great weapon to evolve in modern warfare'.[20] Initially discovered as a side effect of nuclear tests, the phenomenon has now been extended to non-nuclear generators. Such generators can create an EMP which will disable unshielded electronic systems. A development beam generator with a one gigawatt capacity could be used to develop a line of sight

[20] Kopp, C., *A Doctrine for the Use of Electromagnetic Pulse Bombs*, Air Power Studies Centre Working Paper Number 15, July 1993, RAAF Fairbairn; see also Kopp, C., 'EMP - The Emerging Electromagnetic Threat', *Australian Aviation*, July 1995, p 50.

EMP which would knock-out most unshielded electronic devices within a radius measurable in tens to hundreds of metres, depending on the employment method. High power microwaves, communications, computers, navigation and data processing systems would be most affected by such weapons. The current limitations of these weapons are power generation and capacitor storage capability,[21] but these can be expected to be overcome in the future.

Reports indicate that research is well advanced with EMP warheads recently being fitted on USAF air launched cruise missiles.[22] EMP weapons are less discriminatory than HERF guns and could be used to shut down a general area rather than a specific system. Again, with the exception of screening techniques such as Gaussian shielding, defensive measures are not common.

Other Information Weapons[23]

There are several weapons which are currently being developed which do not fit in the HERF or EMP categories. Some already are in service with various military forces, others remain on the drawing board. The following weapons are described in a variety of freely available publications and give an indication of the technologies being developed and the possible capabilities which may result.

Low Energy Lasers. These lasers can be used to damage the optical systems of sensors (including data collection devices), thus attacking the information systems at the data collection level. Low energy lasers have already been fitted on rifles and armoured vehicles and were deployed during the Gulf War. A number of systems are reported to be under further development in the US and UK.[24]

Electrical Power Disruption Technologies. An electric power disruption munition was first used during the Gulf War in 1991. The technology originated after an accident on the US West Coast when chaff cut power supplies to the city of San Diego in 1985. The weapon uses light, conductive, carbon fibres which wrap around transmission lines and distribution points to cause a massive short circuit. Even when power is restored the fibres must be removed because any breeze can result in another short circuit.[25] This weapon can be delivered by cruise missiles, as was the case in the Gulf War, or from manned aircraft.

MIO Summary

Individually, each of the MIO tools and techniques described will present a military commander, whether operating in the conventional or IW environment, with a

[21] Evancoe, P.R., 'Non-Lethal Technologies Enhance Warrior's Punch', *National Defense*, December 1993, p 27.
[22] Fulghum, D.A., 'ALCMs Given Non-lethal Role', *Aviation Week & Space Technology*, 22 February 1993, p 20.
[23] The section on non-lethal weapons is largely extracted from Wing Commander Ric Casagrande, *Non-Lethal Weapons: Implications for the RAAF*, RAAF Air Power Studies Centre, Paper Number 38, November 1995, pp 13-16.
[24] Evancoe, P.R., 'Non-Lethal Alternatives: Weighed by Law Officers', *National Defense*, May/June 1994, p 29.
[25] Starr, *Pentagon Maps Non-Lethal Options*, p 38.

substantial force multiplier. Collectively, they offer a decisive addition to military power. As more MIO capabilities are developed the effectiveness of the MIO strategy will increase exponentially, reflecting the synergistic relationship that exists between individual elements of the MIO environment. Accordingly, nations developing information strategies should consider investment, both intellectually and financially, across the gamut of information operations.

IMPLICATIONS FOR AUSTRALIA

The description of the types of information operations that are currently available should alert military forces to the vulnerability associated with information-dependence in modern conventional warfare. The vulnerability of their national information infrastructure should also be clear. The development of protection devices for modern information systems is significantly behind the development of destruction devices. There is simply no such thing as a 100 per cent secure system at present and this situation is likely to continue for the foreseeable future. [26]

A Third World nation can now purchase information weapons and develop offensive information systems that can potentially do as much harm to an enemy as bombs and bullets, arguably with a higher chance of successful employment. Full incorporation of MIOs into existing conventional military strategies and doctrine, however, will take some time. Therefore, within the known conventional military environment, the Australian Defence Force (ADF) is unlikely to be directly threatened by MIOs in the near future. However, an information attack can be conducted without conventional attacks being mounted, by both nation state and non-nation state entities. This scenario elevates information operations into the paradigm of IW that was briefly discussed early in this paper.

Although detailed discussion of the IW paradigm is beyond the scope of this paper, three general observations should be noted.

a. Harassment via information operations is far easier, more efficient and often politically more acceptable, particularly in the eyes of the international community, than conventional military operations. Therefore, the restraint that is an accepted part of conventional warfare posturing may not necessarily be applied to an information conflict.

b. The more advanced technological nations and military forces are more susceptible to information attacks, as they generally employ and depend on the integrity of multiple complex information systems. Accordingly, the ADF as a technologically advanced military force would be affected by an information attack to a greater degree than many of the regional military forces.

c. If a nation wishes to develop an offensive information strategy against Australia, it does not have to develop its own capability. There are reportedly many information mercenaries who would, for the right price, develop and

[26] Taken from a lecture on IW given by Dr Brian Billard of the Defence Science and Technology Organisation at the Australian Defence Force Academy, 1996.

conduct information attacks on nations. During the Gulf War an organisation known as 'Hi-Tech for Peace' offered their services to Iraq for $1m. Any organisation wishing to develop strategies against Australia would probably need 3-12 months preparation time, if the attack was to be conclusive. For simple harassment, an attack could probably be coordinated in weeks.

THE PRINCIPLES OF INFORMATION OPERATIONS

Eight principles of information operations[27] can be applied either in support of a conventional or a purely information war. These principles are equally applicable to the civilian environment as they are to the military environment. They can be applied as a framework for any nation as it embarks on the development of information security strategies, or to any military as it develops information operations or information warfare strategies. The principles are grouped under three levels of information operations: assurance, superiority, and dominance.

Information Assurance

The primary challenge that must be met by nations and military forces is the protection of their own information infrastructure. This requires knowledge, the development of systems designed to survive, and an understanding of the speed and responsiveness that must be designed into a modern information system.

The Principle of Knowledge. The principle of knowledge involves two separate important issues.

a. Firstly, systems should enable as much information as possible to be made available to those who need it. Information hierarchies insert unnecessary choke points and cannot be efficiently applied to information dissemination in the information age. Networks are the most appropriate form of information distribution.

b. Secondly, system architects, users and warriors will need to fully understand the information environment within which they operate. In particular, they need to clearly understand the capabilities of potential aggressors and their information systems, the availability and applicability of the most capable information tools and techniques, and the vulnerability of their own systems.

The Principle of Survivability. Information policy and strategy should be centralised in order to ensure a national focus that is consistent with broader national objectives and to ensure efficiency in their development, but execution should be decentralised to minimise system vulnerability to an information attack. Planning should empower agencies to undertake specific activities without the requirement for authorisation from any 'higher authority'. If part of the information network is neutralised by an information attack, the remainder must still be able to function. This re-enforces the need for networks rather than hierarchies. If a piece of data is available to everyone,

[27] These principles were adapted from the work of information warfare theorist, Owen Jensen, 'Information Warfare: Principles of Third Wave War', *Airpower Journal*, Winter 1994.

and the agencies are empowered to act on that data, a potential aggressor will be required to target the entire network rather than individual systems or nodes. Nodes should be avoided at all costs. Any single point failures, that is an individual piece of equipment or person that is absolutely vital to success of the system, is a valid and most attractive target. Survivability also requires the application of rigorous analysis of friendly systems, the absolute adherence to protection strategies, and the regular review and upgrading of critical systems.

The Principle of Alacrity. The principle of alacrity states that there must be a tight decision loop and a sense of urgency applied to all information operations and systems, and in particular there must be an inherent ability for a system to rapidly react to changes in its environment. This principle recognises the time sensitive nature of information and is applied to both the processing of data and the human assimilation function. Applied to the design of systems, this principle again stresses the need to avoid hierarchies. A single piece of data should be available to everyone simultaneously. Any modifications to that data can be made by anyone with value to add, and the resultant information should be automatically made available to any user, regardless of her/his place in the organisation or decision making process.

The discipline of assurance is the most critical challenge facing organisations that intend operating in the information age. While the consequences of not being able to attack an opponent's systems are not great, the consequences of not being able to defend one's own are substantial and may ultimately include defeat. The integrity of friendly information systems, and thus information assurance, is the most fundamental discipline of information operations. Accordingly, the first step in the development of any information strategy must be the protection of friendly systems.

Information Superiority

Once the integrity of friendly information systems can be assured, a further option is to expand the influence of the information system into the wider environment within which the organisation intends operating. To achieve this, an organisation should focus on ensuring the primacy of its systems and then induce a potential aggressor to prematurely display its defensive information capabilities.

The Principle of System Primacy. The principle of system primacy states that necessary aggressor systems should be able to be suppressed if the need arises. This requires strategies to be in place which will systematically manipulate aggressor's systems with a view to creating a desired outcome. This demands the identification of the enemy's system weaknesses and strengths and the development of coordinated strategies which allow friendly systems to operate at will within the enemy's information environment.

The Principle of Inducement. Once an organisation is confident that an enemy's information systems can be suppressed, it may wish to induce an initial enemy response to the threat against their information integrity. By forcing an enemy to initiate its defensive mechanisms, friendly information warriors will be able to better analyse the strengths and weaknesses of the enemy's systems and, if necessary, refine their offensive strategies prior to a full scale attack. This will leave the enemy's systems more vulnerable to friendly systems, thereby increasing the chances of

successful engagement. This is similar to the way that naval forces may try and encourage enemy units to leave the safety of a harbour and thus allow submarines to engage. Of course, if the enemy chooses not to engage, the battle may have already been won.

Information Dominance

Once friendly information forces and systems have established information superiority, they will be in a position to prosecute an information campaign should they desire to do so. Successful prosecution requires the decapitation of an enemy's system from those who need the information that the system is producing and the commitment on behalf of the friendly decision makers to ensure that the information attack is decisive.

The Principle of Decapitation. Decision support systems, communications and command and control systems, and essential surveillance, reconnaissance and intelligence systems should be the primary targets of an information campaign. If these systems can be closed down or manipulated to create a desired output, the remaining systems will be of little significance and can be eliminated if required as a second priority. A system that has been disconnected from the decision makers is of little use. Ultimately, an information system, no matter how advanced, must provide an output to a decision maker, even if that decision is being made by another information system. Information operations seek to manipulate, corrupt, destroy or create uncertainty concerning the validity of that output. The information warriors' target is the processes involved in creating the output. They will seek to cut a system into small, useless elements. This is the process of decapitation. If uncontaminated information is denied to the decision maker, the information operation is successful.

The Principle of Intensity. Regardless of the scenario, once a decision has been made to engage in information operations, there should be no limits placed on the operation. Disabling half a system is pointless as most systems will have a degree of redundancy built into them. The enemy's systems must therefore be examined as a whole, with the functionality of the systems being considered the target. Even though the system as a whole must be considered, achieving a successful result may often require physical manipulation of only small parts of that system. A coordinated attack will be designed to completely disable specific systems, a military capability, or indeed a national infrastructure. An information operation that reaches the point where an attack is ordered has clearly escalated beyond the diplomatic stage. Restricting the information operation may have similar consequences to the much publicised targeting restrictions placed on American forces by their political masters during the Vietnam war.

Summary of Principles of Information Operations

These principles have been devised primarily with military operations in mind. The principles are equally applicable to any organisation which engages in conflict in the information age, be it commercially, ideologically or politically motivated. They offer a step by step approach to the application of information operations to a conflict environment. Unless information assurance is attained, information superiority cannot be. Likewise, unless information superiority is attained, information dominance

cannot be. While no organisation in the world at present has attained information assurance, it will occur in the future.

INFORMATION AND THE CONVENTIONAL MILITARY ENVIRONMENT

Generic Military Functions

Existing land, sea and air forces undertake several generic functions. Each arm of the military has given these functions various names, and each particular nation has adapted them to suit their particular circumstance. Figure 3 lists the generic tasks/roles comprising the strategies of each of the arms of the ADF. These are generally consistent with those used by most Western nations.

Information operations will support each of the generic functions (control, strike, deterrence and support) for each of the arms, predominantly by providing information assurance. Indeed, information support operations are becoming a necessary part of all of these functions. In much the same way as air power emerged from a means of simply supporting the surface forces, information forces are now emerging as a potent force in their own right. Information power adds a further dimension to the conventional means of exerting military power.

Table 1 - Conventional Force Functions[28]

LAND Apprehend Lodgement	SEA Command of the Sea	AIR	TYPE OF OPERATION
Contain lodgement	Sea Control	Control of the Air	Control
Protect population and vital assets	Sea Denial		
Intercept and destroy enemy	Guerre de Course	Air Strike	Strike
Deter lodgement	Presence	Deterrence	Deter
	Fleet in Being		
(Support)	(Support)	Air Support	Support

Table 1 depicts the way in which generically the elements of land, sea and air strategies may be grouped into types of operations - Control, Strike, Deterrence and Support. MIOs can be similarly grouped into these categories. Information control within the conventional warfare environment, is clearly an emerging military function. Information operations can also be tasked with both strategic and tactical strike, as well as deterrence. Information deterrence operations can be conducted in a similar way to that of conventional deterrence. By maintaining a visibly capable

[28] Hislop, WGCDR P., 'Aerospace Strategy in the Maritime Environment', a presentation to RAN Staff College, 29 March 1996.

information force and, if necessary, publicly demonstrating that force prior to the onset of hostilities, conflict may be avoided.

All arms of the military forces conduct support operations (for each other as well as for themselves) and strike operations as separate yet integrated tasks. Some of these operations can occur without sea, land and air control, or with only partial or temporary control. For example, before heading into enemy territory, the army's special forces do not wait for land to be taken or for the air force to have control of the air. Similarly, strategic strike aircraft may conduct some operations without total control of the air and submarines will often conduct their operations without control of the sea. Likewise, information control provided in support of an air, sea and/or land campaign can be temporary or limited in degree, if desired. Information control need only be sufficient in the tactical environment to permit other operations to be successfully progressed.

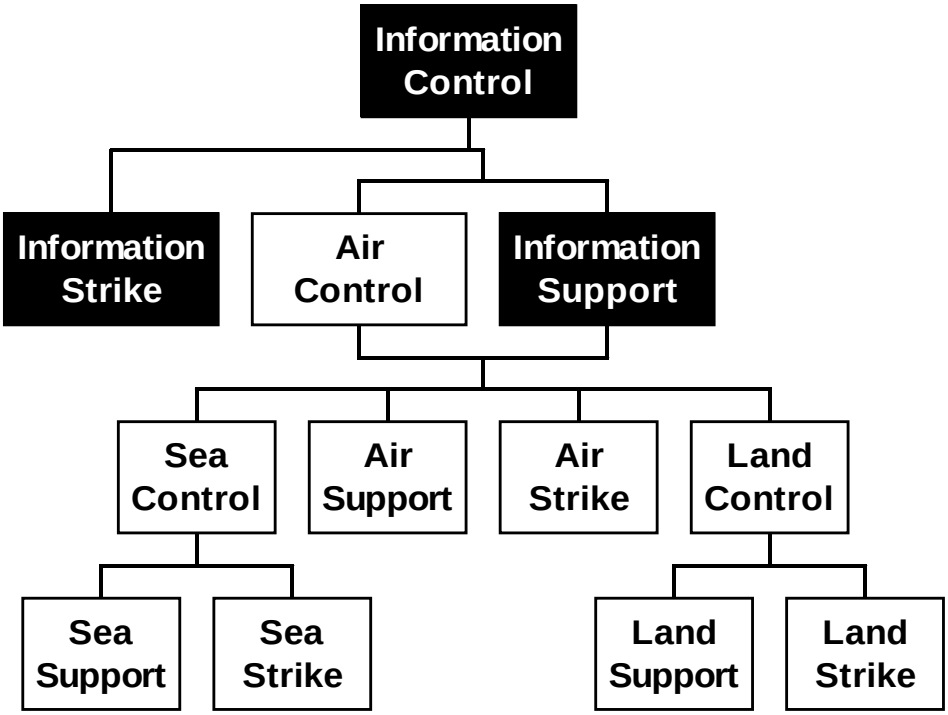

Figure 3 - Conventional Military Roles - Dependency Relationship[29]

Hierarchy of Dependency

Within the broad groupings of military operations in each of the four dimensions of warfare, there exists a hierarchy of dependency where generally one category of operation relies upon at least partial achievement of other types of operation. In general, support operations cannot be conducted in any environment without first achieving at least some level of control. Thus land support operations generally rely on a degree of surface control. This dependency relationship is depicted at

[29] *ibid*.

Figure 3. Deterrence operations are not included in this model because most military operations are coordinated only after deterrence has failed. Within this dependency model, 'conventional' warfare has traditionally recognised the reliance of control in the sea and land environments on control of the air (either actual or by default). However, with the addition of information operations is implied the need for another level in this dependency.

The attainment of control of the air is now as dependent on first having attained control of the information environment as land and sea control are on first having attained control of the air. Without control of the information environment, systems crucial to attaining control of the air, such as command and control, weapons systems and intelligence, surveillance and reconnaissance sensors, may be manipulated or even destroyed by enemy forces. Friendly OODA loops may be subsequently increased and air assets may be subjected to unnecessary risks. Obtaining control of the information environment, therefore, is now a critical task of conventional military forces and features as the first generic function in the hierarchy of dependency.

CONCLUSION

This paper has considered the application of MIOs to the conventional warfare environment. Although the array of MIO tools and techniques have been presented as discrete elements in a schematic diagram, the MIO environment is complex, multi-dimensional, interactive and still developing. Accordingly, the introduction of an MIO capability into an existing military force requires careful consideration and adherence to a series of principles espoused within this paper. These principles are defined within a framework of concepts including Information Assurance, Information Superiority and Information Dominance. This framework can be applied to both the introduction of an MIO capability and the application of MIOs in warfare.

MIOs will change the nature of future wars and will eventually evolve into a separate paradigm of warfare - IW. However, MIOs can be applied to today's conventional environment and it is within this context that more urgent attention from military planners is required. MIOs offer both a support capability to existing arms of the military and also an additional dimension to conventional warfare. They may be used to strike enemy systems, control the overall information environment, deter enemy aggression or support either themselves or other military strategies. Regardless of which tasks they are employed for, MIOs offer a significant addition to the conventional inventory and should be developed as a matter of priority as an essential Joint Force operational capability.