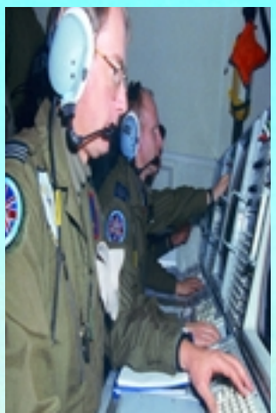
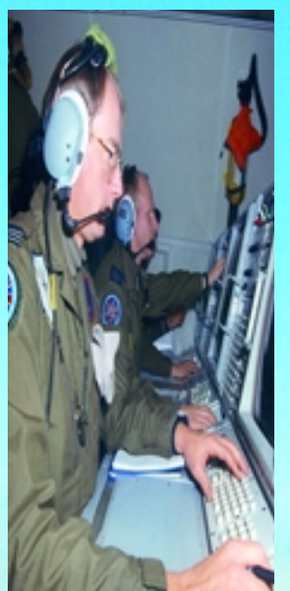
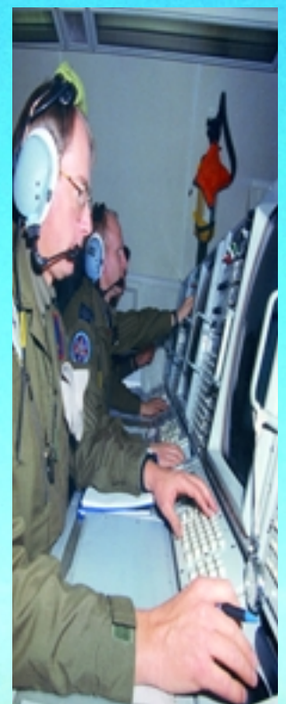
Electronic Fire







By Squadron Leader A J Coller

"War between mass armies weighed down with baroque equipment they cannot use properly has become an established third world sport. The advanced world, too vulnerable to survive a war of attrition or mass destruction, must learn to conduct its affairs by the rapier – by the threat or use of small specialised forces exploiting high tempo and strategic surprise."[1]

Advocates of Information Warfare (IW) talk of a new Revolution in Military Affairs (RMA) that will make current modes of operating and weapons obsolete. In America Andrew Marshall, head of Net Assessment, criticises spending on so-called 'sunset systems,'[2] such as aircraft carriers, tanks and even F-22s'. Modern warfare has become a conflict of 'systems.' Digital networks allow the rapid interchange of data between individual points, around nets, between nets, across the world almost instantaneously and in great volume. In this dynamic systemic environment the effectiveness of violence has been blunted, not because killing the enemy has become any less of a necessity, but because an iron bomb will not easily damage or kill the system or network that guides and directs the energy of a military force. In order to win, and win quickly, pure physical destruction of the enemy is unrealistic and unnecessary. New weapons and new ways of utilising existing weapons are required under new concepts of operations in order to deliver the requisite shock and paralysis to enemy systems to achieve military and political aims.

A REVOLUTION IN MILITARY AFFAIRS?

The Americans are convinced that the RMA is here and are embracing their chosen path to the future, but are they in a 'race of one,' driving forward an unrealistic agenda where the threat is technology itself? The 'information age' has been driven by U.S. industry and research, "*The computer really represents the first genuinely American expression of civilization. More than the auto or television, the computer redefines both thought and daily life. It also will redefine war.*"[3]

More than the auto or television, the computer redefines both thought and daily life. It also will redefine war

Many writers who see the Gulf War as an example of the RMA are often accused of presenting a stereotyped view or of falling for the media image. For Russian observers of the war, it seemed to confirm the early 1980's Soviet prediction of the 'military-technical revolution,' advances in computers, sensors and weapon systems that were expected to inflict damage comparable to that of a nuclear weapon.[4] This was perceived to offer a qualitative transformation in conventional war that would introduce the 'reconnaissance-strike complexes.' What you see in real time you can destroy almost as rapidly, "…operations will no longer be conducted cyclically, with intensive operations followed by lulls. Rather, they will be conducted continuously, making it important to kill an enemy immediately after he is detected."[5] The use of hand held global positioning systems, AWACS, JSTARS, JTIDS, precision guided munitions (PGMs), computerised air tasking orders, all seemed to herald the new dawn. However, whilst many of the components of such a reconnaissance-strike complex were present, there was little integration.

The combat potential of PGMs was first revealed in Vietnam when, on 13 May 1972, 14 bombers dropped both laser-guided and dumb bombs on the bridge at Tanh Hoa finally destroying it after the failure of 871 sorties, the loss of 11 aircraft and the use of 2,000 tons of conventional bombs.[6] During the last decades of the Cold War the USAF began to put faith in such accuracy to counter the Soviet threat. Desert Storm appeared to confirm the power of these weapons, especially when the RAF changed its tactics and adopted the wide scale use of laser guided munitions. Yet a number of reports since the war have played down the significance of PGMs.[7]

The conflict did realise the potential of air power that its pundits had been predicting for so long, even if not in the way that its prophets such as Trenchard or Douhet would have foreseen: as President George Bush said, "Gulf lesson one is the value of air power."[8] But even as air power has come of age, technology has made an even greater impact on the traditional ideas of what is required for victory in the air. 'Stealth' technology was seen as being

…as important as the F-117 was in attacking high-value strategic targets it could neither replace the ordinary bombers nor pave the way for all aircraft in hostile air space

instrumental both in opening the conflict and in neutralising Iraqi air defence systems. Yet as important as the F-117 was[9] in attacking high-value strategic targets it could neither replace the ordinary bombers nor pave the way for all aircraft in hostile air space, "The overwhelming electronic combat achievement laid the basis for all subsequent Coalition military success. Stand-off, barrage and escort jamming of Iraqi radar and fighter control communications blinded and paralysed Iraq's air defence system."[10] The use of AH-64 Apache helicopters to blast a forward air defence radar installation showed both the variety of aircraft types involved in the opening attack and the novel tactical solutions adopted.

The Allies' air and EW campaign turned Iraq's intimidating numbers and hardware into little more than a defenceless and ineffective rabble. In the first hours of the air war, the Iraqi air defences were systematically disrupted. From a front-line strength of around 700 aircraft, the Iraqi air force was to lose only 33 in the air whilst nearly 140 perished in hardened aircraft shelters and more than 120 were eventually flown to Iran.[11] Even so, Coalition planes would not fly missions without SEAD support from US Navy EA-6B Prowlers or USAF EF-111.[12] Such strike support aircraft, and other intelligence-gathering and reconnaissance aircraft, flew more than 50,000 sorties during this short but intensive campaign, such was their crucial importance to the Allies.

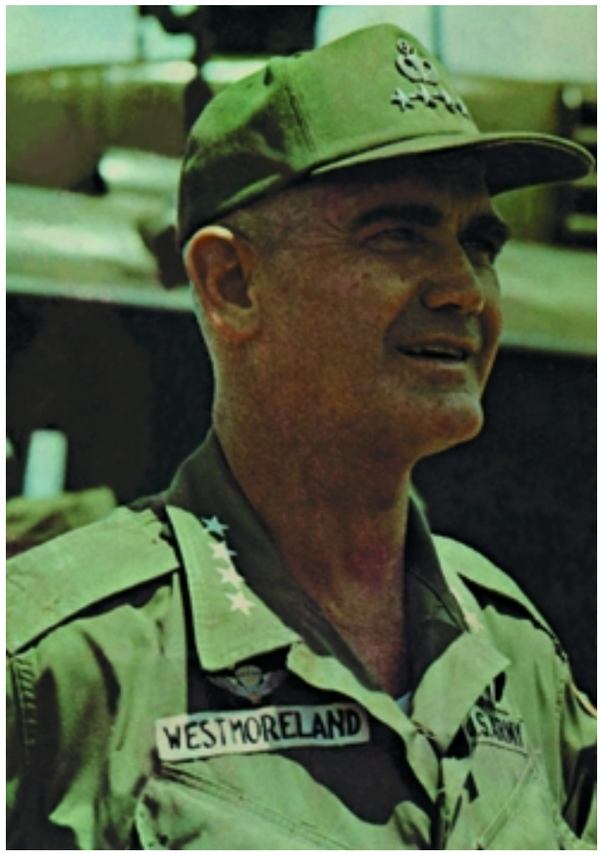
Major General (Retd) Vorobev[13] believed that the eventual land victory had become a certainty as a result of the envelopment of the Iraqis both in the air and in the ether (electromagnetic). He saw the air war in terms of an '*operational electronic-fire battle*' which combined a range of massed, prolonged air and naval, missile and electronic strikes to paralyse and dislocate the Iraqi systems. This symbolism of 'electronic-fire' accords well with the Soviet military's vision of Radioelectronic Combat or Struggle (REB (radioelektronnaya bor'ba)). This aggressive doctrine emphasised the annihilation of enemy command and control systems and structures in order to gain control of the electronic spectrum. While NATO stresses the timely jamming of certain critical radios or radars, the Soviets were more direct. It has been estimated that a goal of the Soviet REB doctrine was to destroy or disrupt at least 50 percent of the enemy's command, control, and weapons systems communications, either by jamming or by destructive fires.[14] They had come to recognise in the early 1970s that in order to off-set NATO's technological superiority they needed to be aggressive in disrupting and denying the electromagnetic spectrum which would allow this superiority to be realised.

It has been estimated that a goal of the Soviet REB doctrine was to destroy or disrupt at least 50 percent of the enemy's command, control, and weapons systems communications, either by jamming or by destructive fires

The Gulf conflict went well for the Coalition for a number of reasons but some were more important than others. The six months of uninterrupted preparation prior to the outbreak of hostilities was a very real advantage; the desert was also an ideal battle space for what was a set piece action, controlled and directed from the centre. The technological one-sidedness meant the question was not who would win but what the price of that victory would be. In the final analysis, numbers aside, the Iraqi armed forces represented a minor power that faced the world's only superpower, and her allies, in a contest where the Allies avoided Iraqi strengths and played to their own.

The Gulf War seems to have reaffirmed the appeal of the technological solution to war but it would be dangerous to ignore the lessons of Somalia or Vietnam. The destruction of the Than Hoa bridge was a success for PGMs; however, its destruction did not prevent NVA supplies getting across the river using prepared fords and under surface bridge platforms.[15] Bosnia and Kosovo have revealed the continuing improvements in the accuracy of PGMs and also their limitations. On balance the conflict saw the application of techniques and weapon systems that had long been available or in development over an extended period of time. But the war did starkly reveal the gulf between the West and even large and apparently well armed Third World armies. If the war was not an RMA then it contained all the elements that will bring about such a revolution in the future.

MILITARY TRENDS



As early as 1969 General William C. Westmoreland was predicting the evolution of an 'automated battlefield'.[16] In this vision of war there would be no need for large forces to fix the opposition physically as the enemy would be tracked and targeted almost instantaneously through use of data links, computer assisted intelligence evaluation and automated fire-control. Vietnam saw the first attempts at realising this approach with the use of ground and air sensors designed to find the Vietcong and then allow their rapid destruction with artillery or air strikes. Westmoreland believed that the sensors were already available for the automated battlefield, but he thought integration was the problem that should be solved in ten years; integration remains a problem both today and for the foreseeable future.

The Westmoreland vision reflects the American dream of a technology driven war with the 'automated battlefield' a centralised quasi-automatic control of war itself. As the pace of war and the destructive power, or accuracy, of weapons increase we become more reliant on machines and there is less room for men. With the increasing employment of machines coupled with the extensive use of modelling there is an inevitable move towards seeing war as capable of being controlled. Man has always sought to impose order on chaos, as much as he has produced that very chaos. During the Second World War modelling was done using real data and it did help in a number of areas.[17] Since then the modelling of possible scenarios has been based on less and less real data and more conjecture or simulation.

The Westmoreland vision reflects the American dream of a technology driven war with the 'automated battlefield' a centralised quasi-automatic control of war itself

Whilst it is natural to seek order from chaos, it is dangerous to believe that war can be ordered. This approach remains susceptible to the same criticisms Clausewitz made of those who sought to reduce war to a set of rules in the nineteenth century. Replacing the war-fighter with more technology will not reduce the dynamics of chaos in conflict and may well increase them. The danger for commanders ensconced in their headquarters viewing neat presentations of maps, units and other information is that computers 'appear' to present an ordered and understandable picture out of a mass of contradictory and fast moving data. That picture is only one version of many possibilities and reflects compromise and limitations in any number of areas, such as programming, available information, the filtering of lower formations and staff officers, etc.

In recent times the battefield has expanded with the capabilities of weapons but the actual battlespace has been reduced. Targets are chosen as much for political or media reasons as for military and the Services must accept a growing political interference down to quite low-levels of detail.[18] The future contains many uncertainties and problems for which a military solution does not exist, such as population growth, immigration, drugs, famine,[19] but this will not prevent the military being fielded to augment political measures.

For the immediate future, the Western trend is toward smaller, professional and more lethal forces equipped with more accurate weapons integrated into advanced C4I systems.[20] Thermal and infra-red night vision and targeting systems will allow forces to operate at both a higher tempo and around the clock. The American domination of space, and her other intelligence and surveillance assets, will provide an 'overwatch' of the battlefield. John Blaker[21] shares Andrew Marshall's view of 'sunset' systems and believes the Pentagon is trying to preserve a force "...designed twenty years ago, for an era that ended nearly a decade ago." In his view the 'big ticket platforms, such as the F-22, draw the lion share of the defence budget and the attention. Blaker would prefer to focus on what platforms carry and the IT that allows the real integration of weapons into a true 'system of systems'. For both Blaker and Marshall, the RMA is all about the interaction of precision, target identification, computers, integration and communications.

The American domination of space, and her other intelligence and surveillance assets, will provide an 'overwatch' of the battlefield

INFORMATION WARFARE

With the advent of the 'Information Age' many of the world's armed forces now rely on the commercial market to provide the majority of their communications bearers and to provide intelligence; from watching CNN to buying satellite imagery. Computers have also allowed other technologies to be developed that have allowed the expansion of the physical battlespace as the potential for military operations can now move beyond traditional boundaries to include virtual economic, financial, psychological, and political targets. The battleground is no longer to be defined by purely geographical boundaries; it extends into 'cyberspace.' Information Warfare is a much-used term of the 90's, but its meaning and impact remains misunderstood.

THE AMERICAN MILITARY CONCEPT OF INFORMATION WARFARE

For the Americans, IW is not something that can be easily defined.[22] Its scope is potentially so broad that it can encompass almost any military action and can, therefore, become almost meaningless as a specific idea. IW, "...is a broad concept that integrates many elements of modern warfare and in fact transcends military applications."[23] The DoD officially defines it as:

> *"Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks."*[24]

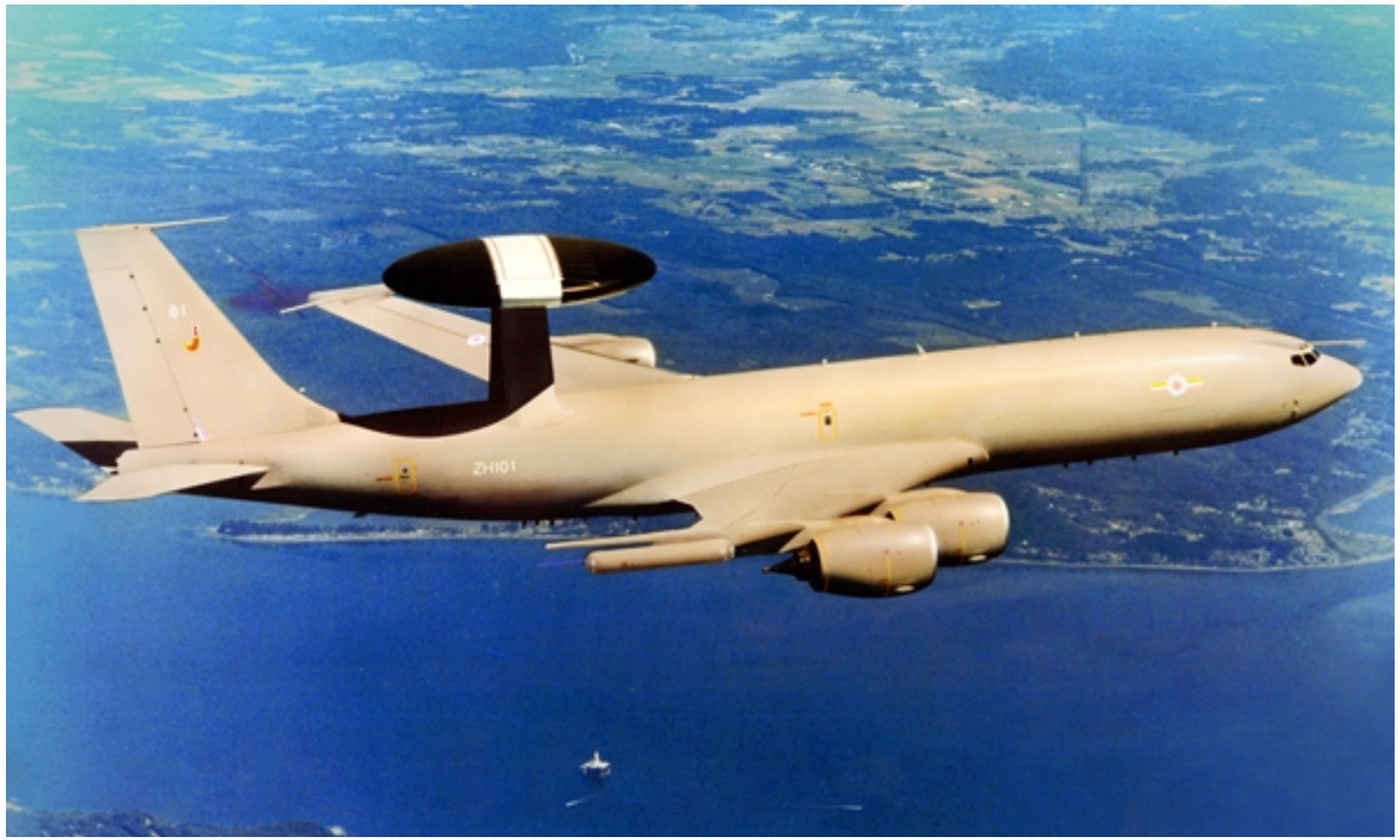
Military IW operations include EW, Psychological Operations, intelligence, etc. Almost any and every action can aid IW operations and objectives from bombing troop positions to using computer viruses to cripple an air defence control system. Traditional weapons platforms equipped with complex computer systems and sensors both demand information (such as JTIDS) and supply it. New technology is blurring once diverse and defining missions. Taken to its logical conclusion, IW is not simply about gaining a better understanding of the enemy and denying him the same, rather it is, "…about influencing human beings and the decisions they make."[25]

American IW is a philosophy rather than a strategy and one that has two sides. First there is the promise of the reduction of the 'fog of war' and the effects of 'friction'. With their control of extensive space and air based sensor and information gathering platforms it becomes almost impossible for the enemy to hide any large force from sight, and with almost real-time data flows it could be possible to launch precision weapons against any detected enemy concentration. Possession of almost unlimited information would allow US forces to dominate any potential battlespace and IW would, therefore, relegate traditional forms of warfare to mere supporting elements of the greater struggle.[26] Conversely, the loss of this information dominance could negate even the strongest military force. The U.S. is most vulnerable to a loss of its information dominance via strikes against the computer networks on which it relies.

The U.S. is most vulnerable to a loss of its information dominance via strikes against the computer networks on which it relies

The American military see IW as being both shaping and paralysing. The former is in its ability to deceive the enemy into acting on or believing false information; the latter when information is used to overload, or is denied to, C4I systems. It is the exploitation of information and information systems to achieve a hitherto unforeseen dominance of the battlespace, both physical and cyber, whilst creating and exploiting the new capabilities and vulnerabilities which accompany this profound revolution. For America, their definition of military IW is C2W.[27] They recognise that digitising the battlespace is not IW. There is a big difference between information-in-war and information, or its denial, used as a weapon.

Admiral William Owens has given the U.S. military a vision of a 'system of systems'[28] which will eventually provide her forces with 'dominant battlespace knowledge' that, when combined with precision stand-off weapons, will allow her to control any given battlespace. In order to achieve this 'system of systems' America needs a 'WarNet'[29] a super C4I data integration[30] of all the various military computers and sensor platforms to provide near real-time situation awareness and reaction. The dream is to own the dimension of time and to be able to control or dominate a situation totally. The power and attraction, therefore, of information dominance is the ability to get inside your enemy's decision cycle; time rather than mere information becomes the new 'centre of gravity.'[31] For IW the primary targets are the C4I nodes, satellites, EW systems and AWACS, not the tank or other weapon platforms which have dominated warfare during much of the twentieth century. This is not to say such platforms have no importance, only that their individual destruction contributes little to the reduction of the enemy 'system'. IW is moving away from the war of attrition towards the incapacitation of the functioning military and political entity.



For IW the primary targets are the C4I nodes, satellites, EW systems and AWACS, not the tank or other weapon platforms which have dominated warfare during much of the twentieth century

ALTERNATIVE APPROACHES TO INFORMATION WARFARE

For the American military definition of IW, information is a target even though information is not an entity, but the information systems can also be a target and they do have a physical existence; the two are differentiated. Information systems can include computers, books, photographs and even human beings. But for the non-U.S. military, IW is perceived as being the threat to computer systems and their data, its loss, copying, corruption or destruction.

Whilst the U.S. military believes there may be a role for new elements, such as viruses, 'herf-guns', hackers, and Trojan horses and does perceive a need to defend its computers against these threats, for many these elements represent the main basis of IW. Cyberspace is regarded as a virtual realm in which little or no law exists to protect the innocent and each firm or government must ensure that its firewalls, passwords and back-up procedures and systems are in place to keep out the unwanted hacker or limit the damage of the unhappy employee or the malicious virus.

The British Defence Doctrine defines IW as:

> *"…actions to attack or defend any of the information-based activities supporting either operational or business processes."*[32]

This definition lacks the broad based philosophy of the American vision. Britain has to date treated the concept of IW with a healthy degree of scepticism,[33] and the MOD has only a limited defensive policy with little concept of the possible threat. Only recently has there been any official recognition that the MOD's reliance on civilian infrastructure and even its own IT systems may be susceptible to a hostile IW attack. At present the MOD has no separate offensive IW policy although it does consider that it is included by C2W.

LIMITATIONS OF INFORMATION WARFARE

Information attacks are not necessarily easy to carry out, especially on a networked system. Dan Kuehl, who is a firm advocate of the potential of IW, is also one of the first to admit that attacks designed to bring down complete systems are not only unlikely to occur but are also beyond most, if not all, countries' abilities. For him IW must be focused to achieve limited aims in association with other weapons in order to achieve the political or military objectives. IW is not seen as a 'silver-bullet', nor is its use expected to be easy.[34] Martin Lubicki has pointed out that IW is extremely difficult to conduct without precise and reliable knowledge of the other side's technical architecture. He draws attention to just how complex this task is becoming as ever more small networked systems are proliferating.

IW operations could view information as the focus or primary target whose destruction or manipulation is seen as the key to success. This approach is dangerous because it transforms information into an entity and a target that can be identified and

"War is an act of force," the very essence of war is fighting and everything else is there either as a prelude, a support or to exploit its outcome

somehow fixed. The proliferation of computers helps to give the impression that information is a centre of gravity, that information is moving from a means to an end. For many in the commercial world information is the be all and end all of IW. Within the military there are many advocates of IW/IO who see information in much the same way, but war is about more than information. "War is an act of force,"[35] the very essence of war is fighting and everything else is there either as a prelude, a support or to exploit its outcome. As with non-lethal weapons, there is an attraction in allotting them a capability for which they either weren't designed or aims for which they were not intended. "The latest batch of cyberwar and information theories are particularly sexy – and dangerously limited."[36] Information is something which is an intangible, you cannot touch it, you cannot be sure it is correct and you cannot be sure what your opponent knows. In the very near future the sheer abundance of commercial satellites and data available on the Internet will make the denial of information to hostile organisations or countries almost impossible.[37] As Lawrence Feedman has noted, with the multiplicity of information channels it becomes almost impossible to stop: "There are few information choke points, no command of info-power easily obtained, no 'centre of gravity' to be targeted."[38]

Instead of information dominance lifting the friction and fog of war we may find that it is supplemented by an 'Electronic fog-of-war.' All concepts of military IW/IO suffer from the problem of obtaining accurate and timely battle damage assessment (BDA). How can cyberwar effects be accurately and timely applied or their effects predicted? Even where successful, for how long will such effects last? It is difficult to ensure that a virus will bring down a system at the right time; too early and back up systems will be activated, too late and the attack has failed. Even with the 'system of systems' the challenge of accurately collecting and analysing information remains formidable. Obtaining the correct data does not guarantee that the commander will receive it, after software and human filtering, or that the right conclusions will be drawn from it. Information fusion and filtering all carry risks, as does the danger of greater centralised control stifling lower echelon initiative or allowing greater political interference. Information dominance presents many individual and organisational challenges for the military staff of the future.

Then there is the simple problem of acting on the data received. During the Gulf War, SCUD hunting had the highest priority, yet reaction time from detection to aircraft on target was about fifty minutes. It took 20 minutes

During the Gulf War, SCUD hunting had the highest priority, yet reaction time from detection to aircraft on target was about fifty minutes

to erect a launcher and only 6 minutes to be on the move again. No kills of mobile launchers were ever confirmed.[39] The Allies lacked the ability to truly watch and react instantaneously. The problem with complete information becomes the speed of analysis and reaction. Even today, intelligence only minutes old may become worthless.

The techniques of cyberwar remain in their infancy and are not widely available within military communities, even in America.[40] IW/IO may not contribute as much in OOTW as some hope; its deterrence value may not be great where visual capability is often the most important factor. IW/IO operations will also be subject to spoofing, deception and other counter-measures. IW offensive and defensive moves will be rapid. By the very nature of digital communications and instructions, this rapidity will be too fast for human cognition if it is to be effectively countered; therefore, a greater level of computer directed automatic defence and counter moves will be required. Another step towards the automated battlefield.

A NEW IMPERATIVE

"It was always clear that the next war would be won by the side which best used the electromagnetic spectrum. In that environment the advantage enjoyed by the power(s) with superior technology over a slightly inferior adversary has probably increased."[41] Today, and even more so in the future, commanders will need to shape the electromagnetic battlefield just as they have shaped the physical one. C2W has the potential to disorganise the enemy, prevent him massing troops or directing effective fire. However, it doesn't go far enough. Russia, in adopting REB, has recognised *"…the increased importance of systems, have focused more attention on the interaction of combat systems instead of on simple force (the old correlation of forces) ratios... According to this logic, warfare is viewed as the interaction among the military systems of the sides in confrontation."*[42]

"The real purpose of heavy weapons is not to destroy enemy soldiers but to destroy enemy weapons. The rationale for this is, if our weapons can shatter the enemy's tanks, artillery, and other guns, then the enemy soldiers will be defenseless, and either be killed or wounded, or forced to surrender or flee."[43] EW can achieve this, temporarily, through jamming. Offensive targeting of electronic transmitters, using anti-radiation missiles or even conventional munitions, can also achieve this aim. Modern weapons are complex inter-linked systems, and quickly become worthless or vulnerable targets without their electronic systems. Spending money on combat platforms gives the public something to show for their money, but without comprehensive EW systems they may truly be 'sunset' weapons. EW, *"…is now so integral to effective war-making that it is difficult to isolate and analyze it as a separate entity."*[44]

In tomorrow's conflicts the side whose systems fail will lose the ability to control not only his own forces but also the ability to shape or influence the battle. In the future we may be able to move away from an emphasis on physical destruction to collapsing the enemy from the inside. Warden's post-Clausewitzian viewpoint recognised that air power could strike, simultaneously against an enemy's entire range of tactical or strategic targets, his five-ring model.[45] Targets should be identified

that can cause the collapse or paralysis of the system and the quickest way is to attack such targets simultaneously across all five rings; 'parallel attack' to cause rapid and real system shock. "Parallel war brings so many parts of the enemy system under near-simultaneous attack that the system simply cannot react to defend or to repair itself. It is like the death of a thousand cuts; any individual cut is unlikely to be serious." That such attacks can be possible despite ever fewer aircraft is due to the availability of accurate weapons which make economy of force possible. However, identifying targets or the centre of gravity requires good intelligence and planning, commodities that may not always be available. Even in the Gulf much of the targeting of Iraqi forces took place before a centre of gravity was identified and was often influenced by political rather than military concerns.[47]

…in the Gulf much of the targeting of Iraqi forces took place before a centre of gravity was identified and was often influenced by political rather than military concerns

As operations speed up traditional command lines are too slow and unresponsive, more devolved command is required, and time becomes ever more important. IT compresses this duration and any degradation in the speed of the process or a return to relying on human links would be a fatal consequence for a modern force in a general war confronting similar conventional forces. The lethality, speed[48] and scope of war have increased, and continue to increase. The difference between the quick and the dead is very small: disrupt the enemy's system and integration collapses. Control of the electromagnetic spectrum is essential if small Western technology-reliant forces are to operate successfully in the future; any disruption could produce a disproportionate effect on the efficiency of such forces. Offensively, it should also be possible to combine the flexibility of air power with the weakness of modern industrial societies and other military forces' reliance on a single technology: the 'chip'. IW, in its broadest sense, seeks to maximise advantages of the information age whilst denying/de-grading it to the enemy. Speed of

The lethality, speed and scope of war have increased, and continue to increase. The difference between the quick and the dead is very small: disrupt the enemy's system and integration collapses

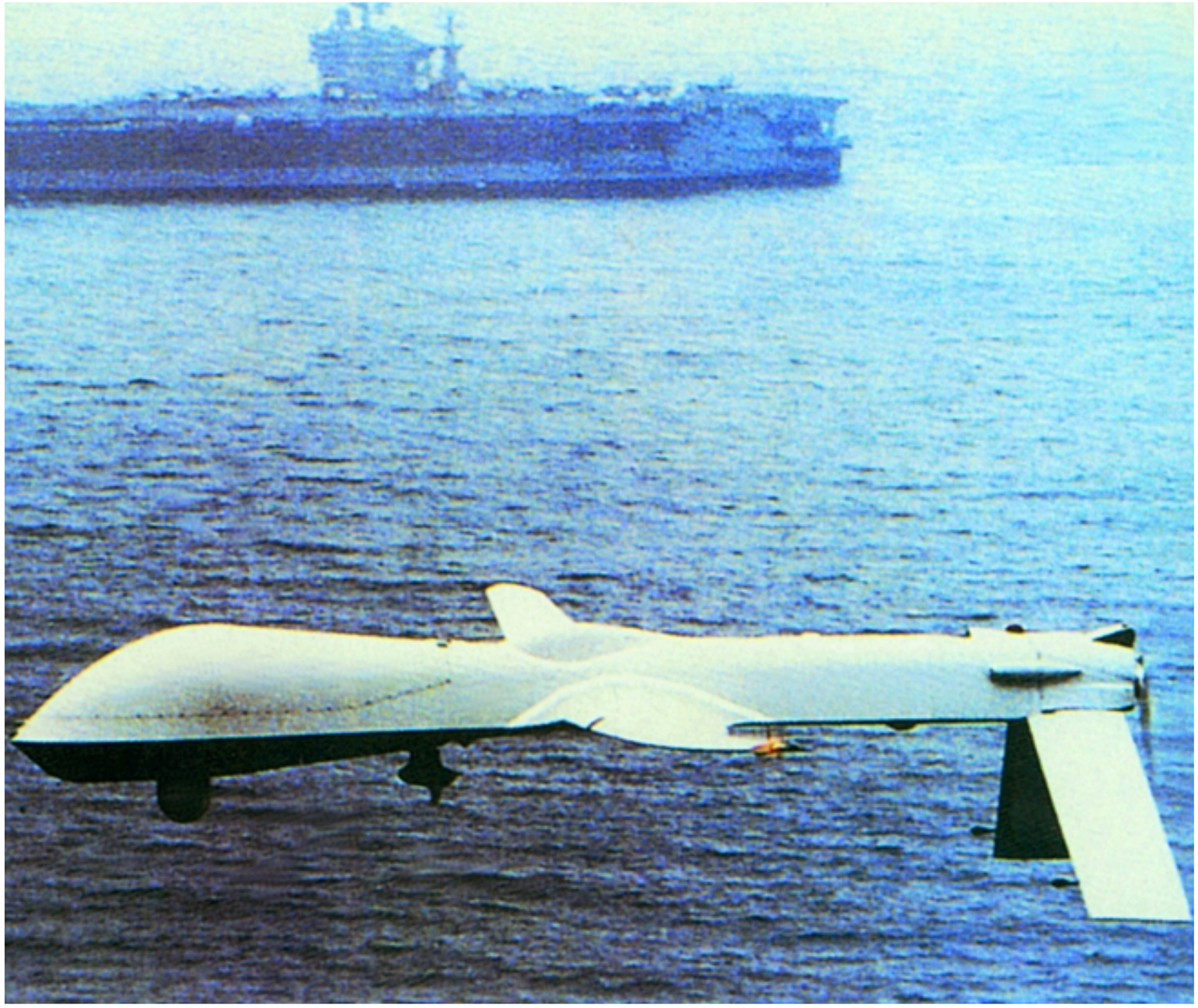
change, speed of response, economies of effort, are today dependent on the exploitation of the chip. Whole 'system of systems' do not need to be completely destroyed but their components and how they interact must be understood if suitable system shock is to be induced. By system shock we must include not only component destruction, loss or denial but also personal shock, confidence in the system (and its information) loss. The human operator and user remains central to any debate in modern warfare, as the American debate on IW/IO recognises and seeks to exploit.

DIRECTED ENERGY WEAPONS (DEWS)

Offensive EW, or electronic fire, requires suitable weapons; existing ARMs are relatively limited in their target set and are reactive in nature. Conventional weapons can be used to hit communication nodes and other electromagnetic targets. DEWs would not replace such weapons; they would complement them. Their scope is enormous as transistors form the core of virtually every modern electrical system from communications to ignition systems. Such transistors are vulnerable to heat and high energy, whether that is radiation or voltage. The Russians believe that REB has become a new combat category and their literature talks of "electronic fire;"[49] DEWs would make the fire real. Dominant firepower leads to domination of the battlefield but traditional concepts of firepower are changing.[50] DEWs could be used to disrupt the entire range of an enemy's system by attacking any and all aspects of the adversary's electrical or digital systems including communications, GPS, targeting systems, radars, fuses, engines, even watches.

There are three general classes of DEWs: lasers, radio frequency (RF) including high-power microwaves (HPM), and energy particle beams. DEWs may be some years away from introduction into service, but they are already available in trial form.[51] The USAF have been testing HPM generators on CMs for some years now, although they have experienced some problems with the range and focus of emissions.[52] The potential power of such weapons has led to some commentators seeing them as destructive as nuclear weapons against electronic equipment: an alternative to the neutron bomb without the nuclear.[53] DEWs also represent a greater threat than conventional weapons due to a number of factors including the higher probability of hit compared with conventional missiles or bullets (an RF weapon is an area weapon); as a result it requires less accuracy and has an instantaneous time of flight. Initially, DEWs are likely to be relatively crude and consist of single emission types mounted

The USAF have been testing HPM generators on CMs for some years now…



Initially, DEWs are likely to be relatively crude and consist of single emission types mounted in CMs, bomb cases or UAVs

in CMs, bomb cases or UAVs.[54] But large aircraft carrying sufficiently powerful generators for a directed HPM beam weapon could enter the tactical as well as strategic arena by being amongst the first to carry reusable DEWs.

Today, electronics are vulnerable to microwaves which can enter systems through either front or back door paths at frequencies that may be either in-band or out-of-band. As components continue to be miniaturised they become more susceptible to HPM; therefore the most modern electronic systems are also the most vulnerable. Protection is possible, but it is difficult to implement and maintain against an unknown range of potential threats. The cost of protecting in-service equipment would be very expensive and may prove impossible to achieve.[55] Simple economics, use of COTS[56] equipment, and normal budgetary pressures will largely negate attempts to design protection for all possible combinations of microwave frequency, bandwidth, pulse width, peak power, and so on. Effective protection for the diverse and widespread electronic systems in use today, against an equally unpredictable threat, is not really a practical option.

Defence suppression is becoming ever more problematic as the increasing sophistication and density of some of the potential threats are making such systems as ALARM and HARM less effective

Defence suppression is becoming ever more problematic as the increasing sophistication and density of some of the potential threats are making such systems as ALARM and HARM less effective. The ability to operate aggressively and successfully in the electromagnetic environment can reduce the reliance on other technologies. If you have other ways to defeat air defences then the need for 'stealth' aircraft is much reduced and simply adopting limited stealth measures, and appropriate tactics, will still allow success in operations. "In the case of RF weapons, if the location of air defense radars and/or C3I systems can be localized (order of kilometers), the potential exists to suppress those sites using an RF weapon to destroy air defense radars/C3I systems electronics."[57] Nor does it matter if the equipment is switched off at the time of the attack.

DEWs have the potential to significantly alter the scope of the future air battle. Indeed, offensive EW can blur the distinction between strategic, operational and tactical still further as DEWs can threaten missile systems as easily as a power grid or banking system. Areas of a nation, from the front-line to the heart of government, would be susceptible to 'electronic fire.' Targets and effects will still be localised and will depend on aircraft, weapons, objectives and time available, but with the

dependence of society on a single vulnerable technology, shock would be assured. Although talking about the use of reserves Col Warden makes a point that is equally valid to the likely effects of DEWs, "...the mental shock to the enemy may be more important than the physical effect..."[58] People are not the direct target of 'electronic fire' but their inability to utilise modern weapons systems will negate their ability to effectively react to or defeat their opponents' weaponry.

People are not the direct target of 'electronic fire' but their inability to utilise modern weapons systems will negate their ability to effectively react to or defeat their opponents' weaponry

A NEW APPROACH TO THE FUTURE

EW and IW are about superiority and denial: the former of the electromagnetic spectrum and the latter of information. Conventional weapons cannot achieve the same effects in either the same time frame or with such few assets. A radically different approach to EW to produce an offensive doctrine of 'electronic fire' can exploit a new philosophy, one that changes traditional views on operations and targeting strategy. It is about how to meet the challenge of the 'information age' and exploit its technology, using a weapon that seeks to rupture, shock and paralyse the enemy's systems by denying them the freedom to operate in the electromagnetic spectrum whilst assuring our own exploitation of this medium.

An aggressive EW doctrine utilising DEWs would find them a flexible tool, a media friendly weapon. They allow damage without great physical destruction or loss of life. As Third World countries continue to buy advanced weapons it is necessary to accept that whilst few really have the ability or the money to maintain extensive C4I systems, sensors and EW systems, they do represent a threat to our ability to operate freely. The psychological effects of losing systems to DEWs and the jamming of others would be a serious blow to such forces and their politicians. Control of the electromagnetic spectrum cannot assure victory against a less advanced opponent but it can deny them the ability to utilise more advanced weaponry.

Although not discussed, DEWs also have a defensive function disrupting, by whatever means, the target-tracking capabilities of autonomous or semi-autonomous weapons. An optical seeker may not be fooled by IR flares or towed decoys, but if its computer guidance system is scrambled it will probably fail. An anti-aircraft system based on DEWs will also knock an aircraft out of the sky as easily as a missile if it flies into its zone of effectiveness. However, the down side to such weapons is the chance of fratricide against your own systems.

An optical seeker may not be fooled by IR flares or towed decoys, but if its computer guidance system is scrambled it will probably fail

Conventional weapons can strike, albeit less effectively, at electromagnetic spectrum targets. There is jamming, both stand-off and platform defence, but counter measures cannot easily defeat multi sensor types and C4I systems with fallback facilities nor jam resistant communications. DEWs do not need to remain up-to-date with frequency changes or ECCM techniques; they will simply destroy the electronic components. Danial Deudeney, an American expert in Information technology, has suggested that "Advances in IT – sensors, communications and data processing – have created a rudimentary planetary nervous system, fragments of a planetary cybernetic."[59] The life blood of such a cybernetic remains the electromagnetic spectrum. IW attacks part of its functions, the brain and sensors, but offensive EW or electronic fire could be the nerve-agent that paralyses and slows the system down leaving it vulnerable to attack.

Electronic fire is not necessarily the right or, indeed, the only choice for the future but control of the electromagnetic spectrum is essential for modern forces and it is a weakness the RAF has recognised. It is an area which is also the bedrock underlying the information age and its technology. So while there are other choices that can reasonably be made or argued for, an enhanced and expanded EW doctrine represents a promising possibility for the RAF. The interplay between doctrine and technology is complex; it is not a straightforward matter of establishing operational requirements, it should also involve experimentation and innovation. The promise of the new digital driven RMA is the ability to conduct operations, albeit adhering to traditional military rules, in a completely new way. The integration of not only weapon systems but also support areas, of all land, sea and air forces, into a single, operational system will require new organisations and flexibility. Above all, the ability to dominate the electromagnetic spectrum will confirm the necessary skills and capabilities needed to operate in the twenty-first century and provide the foundation for building upon new technology and concepts as they become available.

"The common thread throughout...is the emphasis on the need to examine the manner and extent to which information technologies alter our basic assumptions about the nature and conduct of war."[60]

NOTES

1 Simpkin R., *Race to the Swift,* p. 180.

2 Ascribed to Marshall by Dr Libicki, at National Defense University (NDU), 28 May 1998.

3 Friedman, George & Meredith, *The Future of War: Power, Technology & American World Dominance in the 21st Century.*

4 Fitzgerald Mary C., 'The Soviet Image of Future War: Through the Prism of the Gulf War', pp. 4, 66-67. Maj Gen(Reserve) I. N. Vorob'ev, Doctor of Military Science, 'Lessons of the War in the Persian Gulf', saw the Gulf as an RMA in the same vein as the Franco-Prussian War, the latter exhibited the changes in small arms, open-order infantry tactics, railway and telegraph. The former showed the face of twentieth century warfare.

5 Thomas T. L., *Dialectic Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations,* p. 14.

6 Werrell K. P., 'Did USAF Technology Fail in Vietnam?', pp. 87-99.

7 The US General Accounting Office , *Operation Desert Storm: Evaluation of the Air campaign,* suggests that the DOD, and several contractors, over-emphasised the contributions of stealth and laser-guided bombs as factors in the success of the air campaign and have given very little credit to less publicised systems. Keaney T. A. & Cohen E. A., *Gulf War Air Power Survey Summary Report,* accept that the PGM success came as a surprise to the Americans, as much as the Iraqis, and that they did have limitations. It was their combination with stealth that made them so effective initially and then the absence of any real Iraqi threat to Coalition aircraft that allowed their unrestricted use. PGMs were not revolutionary, as they had been used extensively in Vietnam during the Linebacker operations; rather it was the quantitative increase in their use that was new.

8 Nalty B. C. (Ed), *Winged Shield, Winged Sword: A History of the United States Air Force,* Vol. II 1950-1997, p. 565.

9 Keaney T. A. & Cohen E. A., *Gulf War Air Power Survey Summary Report*, the F-117s flew only 2% of the total attack sorties, yet hit nearly 40% of the strategic targets.

10 Mason T. – *Air Power A Centennial Appraisal.*

11 Cohen E.A., 'The Mystique of U.S. Air Power'.

12 Watson B. W. (Ed), *Military Lessons of the Gulf War.*

13 Vorob'ev .I. N., Maj Gen(Reserve), Doctor of Military Science, `Lessons of the War in the Persian Gulf'.

14 See Munro N., *Electronic Combat and Modern Warfare: The Quick and the Dead* and Chizum D. G., *Soviet Radioelectronic Combat.*

15 Werrell K. P., 'Did USAF Technology Fail in Vietnam?', pp. 87-99.

16 Cliffe T. , 'Military Technology and the European Balance', pp. 1-58.

17 Ibid. Mathematical modelling techniques helped to achieve an increase in the kill rate of U-boats by a factor of 3 as the modelling allowed the isolation of significant variables, i.e., large convoys were better than smaller convoys, identification of optimum search patterns and fuse settings.

18 Gray C. H., *Postmodern War: The New Politics of Conflict*, has highlighted this paradox of capability restricted by the political decision rather than by actual ability.

19 Barnaby F., *The Automated Battlefield.* The population of the industrialised countries is approximately 1,200 million and is likely to remain around this level; that of developing countries may reach 10 billion by 2030. Environmental threats, global warming and the widening poverty gap between rich and poor will all impose strains in future relationships that may fracture into armed conflict.

20 Starr B., 'USA's rapid targeting reaches new heights', pp. 22-23. The Rapid Targeting System (RTS) architecture aims to transmit real time imaging data to aircraft; brings the 'reconnaissance-strike complex' closer to realisation. "The aim is to provide real-time information into the cockpit of F/A-18 Hornet and F-15 Strike Eagle aircraft for attacking mobile targets such as 'Scud' launchers within five to 10 minutes..."

21 Blaker J. R., 'The American RMA Force: An Alternative to the QDR', p. 21-30.

22 *Air Force Basic Doctrine,* talks about Information Operations (IO) which are defined as, "Those actions taken to affect adversary information and information systems while defending one's own information and information systems." IW is referred to but it is IO on which the doctrine concentrates. Libicki M. C., *What Is Information Warfare?*, "...information warfare may better be considered a mosaic of forms, rather than one particular form."

23 Harley J. A. Lt Cdr USN, 'Information, Technology, and the Center of Gravity', p. 68.

24 *Joint Publication* 1-02, Department of Defense. The USAF, *Air Force Basic Doctrine*, includes a copy of this definition plus an additional definition for clarity, "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".

25 Stein G. J., 'Information Warfare', p 124.

26 Chairman of the Joint Chiefs of Staff, National Military Strategy (February 1995),p.15, "winning the information war" is a priority.

27 Campen A. D. (ed), *Cyberwar: Security, Strategy, and Conflict in the Information Age*, the Joint Chiefs of Staff have said that C2W is the military component of IW (JCS Memorandum of Policy (MOP) 30),it has 5 elements deception, operational security(OPSEC), EW, Psychological Ops and physical destruction.

28 Owens William A., 'The Emerging System of Systems', p 15-19.

29 Thomas Timothy L., 'The Threat of Info Operations: A Russian Perspective' in Pfaltzgraff Robert L., Jr & Shultz Richard H., Jr (eds), *War in the Information Age.*

30 Evers S., 'Data fusion holds the key to US 2025 vision', p.27. 10 person team paid to 'free-think' possibilities for the future of war have identified data fusion as one of the most pressing of requirements.

31 John R. Boyd's Observation, Orientation, Decision, Action (OODA) loop has become a popular American model for describing the decision making loop: he uses it to describe the interaction with the environment and sensory data. U.S. forces want to have a smaller OODA loop than their potential opponents. Boyd's work is much quoted by current American military writers, especially on IW, but his work remains unpublished.

32 *British Defence Doctrine,* (JWP) 0-01, p. 4.10.

33 European armed forces have traditionally been less dependent on technological solutions in war and are, therefore, less technologically focused than America.

34 Interview with Dr Dan Kuehl at NDU, 28-29 May 1998.

35 von Clausewitz C., *On War*, p. 77.

36 Gray C. H., *Postmodern War: The New Politics of Conflict*, p. 23.

37 A U.S. Army wargame revealed this dilemma when players were attempting to deny or subvert intelligence sources on which a future enemy was relying and utilising, reported by Seffers G. I., 'Army War Game Reveals Power of Commercial Data', p 44.

38 Freedman L., 'Information warfare: will battle ever be joined?', p. 98.

39 Shukman D., *The Sorcerer's Challenge: Fears and Hopes for the Weapons of the Next Millennium*.

40 Fulghum D. A., 'Cyberwar Plans Trigger Intelligence Controversy', pp. 52-54. Intelligence agencies are restricting the USAF's ability to hack into enemy systems. The secrecy that surrounds such techniques mean that they are currently unavailable to commanders in the field; similarly, during the Gulf, they were either not revealed or offered too late to make any difference. The military reportedly remain lacking even a working knowledge of true capabilities thus restricting their ability to conduct realistic desk-top exercises.

41 Bellamy C., *Expert Witness: A Defence Correspondent's Gulf War 1990-91*, p. 176.

42 Thomas T. L., *Dialectic Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*.

43 Alexander B., *The Future of Warfare*, p. 65.

44 Watson B. W. (Ed), *Military Lessons of the Gulf War*, p. 163.

45 Warden III, Col J., 'The Enemy as a System', pp. 364-374.

46 Warden III, John A., 'Air Theory for the Twenty-first Century', from Magyar K. P.(Ed), *Challenge and Response: Anticipating US Military Security Concerns*.

47 De La Billiere, General Sir Peter., *Storm Command: A Personal Account of the Gulf War*, “By the third day of the war we were putting forty per cent of all our air sorties into our effort to destroy the (SCUD) launchers…”.

48 At a pre-war conference, German Air-force General Erhard Milch said, “The real secret is speed – speed of attack through speed of communication.” Keegan J., *A History of Warfare*.

49 Kipp J. W., ‘Confronting the RMA in Russia’, pp. 49-55.

50 Shukman D., *The Sorcerer's Challenge: Fears and Hopes for the Weapons of the Next Millennium*. He suggests that an electromagnetic weapon weighing 10-40 pounds could give off 100 megawatts in a single flash effective to out to 4 kilometres, more than enough to ‘fry’ most transistors. Another example of a possible DEW is an isotropic radiator – a 'light bomb', which would be capable of producing an incredibly powerful flash that could temporarily blind all optical devices.

51 Starr B., *Russian bomb-disarming device triggers concerns*, p.4. Russia has developed “...a compact high-current electron accelerator that could potentially stop car engines and destroy the electronic arming and firing circuits of bombs.” Called the RADAN, it is smaller than an attaché case, weighs about 8kg and has a directional antenna and a 12V rechargeable battery. Dr Ira Merrit, of the advanced technology directorate at the US Army Missile Defense and Space Technology Center. Congressional Joint Economic Committee (JEC). US scientists have long been monitoring Russian, French and Swedish programmes. “France's Gramat Research Centre ‘has dedicated significant assets to study the effects of electromagnetic energy on electronics’” according to Dr Merrit's statements.

52 Fulghum D. A., ‘New Weapons Slowed By Secrecy Clampdown’, pp.54-56. The USAF also contend that future improvements may allow the YAL-1A airborne laser (ABL) to be used in the SEAD role by disabling electronic equipment in air defence sites.

53 DoD, *Critical Technologies Plan*. “High power microwave weapon offers a revolutionary means of defeating enemy weapons in mass. It may also provide means of severely interrupting enemy communications….without resort to the nuclear arsenal.”

54 Fulghum D.A., ‘Computer Warfare Offense Takes Wing’, pp. 56-58. UAVs and stand-off missiles are being developed as EW platforms. “Teledyne Ryan Aeronautical is preparing some of its Model 350 (BQM-145) fleet of high-speed, swept-wing, medium-range UAVs for installation of a directed energy weapon - perhaps a laser or HPM device – for an unnamed customer.”

55 Baker Dr. William L., ‘Air Force High-Power Microwave Technology Program’, pp.13-17.

56 R. P. O`Neill, ‘Integrating Offensive and Defensive Information Warfare’ in Pfaltzgraff Robert L., Jr & Shultz Richard H., Jr(eds), *War in the Information Age*. Civil sector advances are now out-pacing military development in all but the most specialised of fields: “Market realities yield a policy encouraging purchase of commercial off-the-shelf (COTS) equipment for military procurement”.

57 Marquet Dr. Louis C., Assistant Deputy Under Secretary for Advanced Development, OUSD/A&T, ‘Aircraft Survivability and Directed Energy Weapons’.

58 Warden III J. A., *The Air Campaign: Planning for Combat*.

59 Barnaby F., *The Automated Battlefield*, p. 38.

60 Pfaltzgraff Robert L., Jr & Shultz Richard H., Jr (eds), *War in the Information Age*.

BIBLIOGRAPHY

Alexander B., *The Future of Warfare*. W. W. Norton & Company Inc, New York and London, 1995.

Barnaby F., *The Automated Battlefield*. Sidgwick & Jackson, London, 1986.

Bellamy C., *Expert Witness: A Defence Correspondent’s Gulf War 1990-91*. Brassey`s, London & New York, 1993.

Campen A. D. (ed), *Cyberwar: Security, Strategy, and Conflict in the Information Age*. AFCEA International Press Fairfax, Virginia, 1996.

Chizum D. G., *Soviet Radioelectronic Combat*. Westview Press/Boulder and London, 1985.

Clausewitz C. von, *On War*. Edited & Translated by Michael Howard & Peter Paret, Princeton University Press, New Jersey, 1976.

De La Billiere, General Sir Peter., *Storm Command: A Personal Account of the Gulf War*. HarperCollinsPublishers, London, 1992.

Friedman, George & Meredith., *The Future of War: Power, Technology & American World Dominance in the 21st Century*. Crown Publishers Inc, New York, 1996.

Gray C. H., *Postmodern War: The New Politics of Conflict*. Routledge, London, 1997.

Keaney T. A. & Cohen E. A., *Gulf War Air Power Survey Summary Report*. Department of the Air Force, Washington, D.C., 1993.

Keegan J., *A History of Warfare*. Hutchinson, London, 1993.

Mason T., *Air Power A Centennial Appraisal.* Brassey`s, London & Washington, 1994.

Munro N., *Electronic Combat and Modern Warfare: The Quick and the Dead*. Basingstoke, Macmillan, 1991.

Nalty B. C. (ed)., *Winged Shield, Winged Sword: A History of the United States Air Force*. Air Force’s History and Museums Program, USAF, Vol. II 1950-1997, Washington, D.C., 1997.

Pfaltzgraff Robert L., Jr & Shultz Richard H., Jr(eds)., *War in the Information Age*. Brassey`s, Washington & London, 1997.

Shukman D., *The Sorcerer’s Challenge: Fears and Hopes for the Weapons of the Next Millennium*. Hodder & Stoughton, London, 1995.

Simpkin R. E., *Race to the Swift: Thoughts on Twenty-First Century Warfare*. Brassey`s (UK) London 1985.

Thomas T. L., *Dialectic Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*. Conflict Studies Research Centre Foreign Military Studies Office, Camberley, England, July 1997.

van Creveld, Martin., *On Future War*. Brassey`s, London, 1991.

Warden III J. A., *The Air Campaign: Planning for Combat*. National Defense University Press, Washington, 1988.

Watson B. W. (ed)., *Military Lessons of the Gulf War*. Greenhill Books, London and Presidio Press, California, 1993.

OFFICIAL PUBLICATIONS

British Defence Doctrine, Joint Warfare Publication (JWP) 0-01. MOD CS(M)G, London, 1996.

Air Force Basic Doctrine, Air Force Doctrine Document 1, September 1997, US Dept. Air Force

Joint Chiefs of Staff, DoD Dictionary of Terms, Joint Pub 1-02, US Government Printing Office, Washington, D.C., 1994.

New World Vistas: Air and Space Power for the 21st Century, Summary Volume, US Dept. Air Force, 1995.

Operation Desert Storm: evaluation of the air campaign, Washington, D.C.: United States. General Accounting Office, 1997

ARTICLES

Baker Dr. William L., 'Air Force High-Power Microwave Technology Program', *Aircraft Survivability Newsletter*, (Fall 1995), Air Force Phillips Laboratory, Kirtland AFB, NM, 9-15.

Blaker J. R., 'The American RMA Force: An Alternative to the QDR', *Strategic Review*, (Summer 1997), 21-30.

Cliffe T., 'Military Technology and the European Balance', *Adelphi Papers*, No 89, The International Institute for strategic Studies, (1972), 1-58.

Cohen E.A., 'The Mystique of U.S. Air Power', *Foreign Affairs*, (January/February 1994),Vol. 73, No. 1, 109-124.

Evers S., 'Data fusion holds the key to US 2025 vision', *Jane's Defence Weekly*, Vol. 28, No 6, (13 August 1997), 27.

Fitzgerald Mary C., 'The Soviet Image of Future War: Through the Prism of the Gulf War', *Hudson Institute*, HI-4145, (May 1991), 4 & 66-67.

Freedman L., 'Information warfare: will battle ever be joined?', *Defence Systems International,* 95-98.

Fulghum D. A., 'Cyberwar Plans Trigger Intelligence Controversy', *Aviation Week & Space Technology*, (January 19, 1998), 52-54

Harley J. A. Lt Cdr USN, 'Information, Technology, and the Center of Gravity', *Naval War College Review*, Vol. 1, No 1, 66-87.

Kipp J. W., 'Confronting the RMA in Russia', *Military Review*, (May - June 1997), 49-55.

Marquet Dr. Louis C., Assistant Deputy Under Secretary for Advanced Development, OUSD/A&T, 'Aircraft Survivability and Directed Energy Weapons', *Aircraft Survivability Newsletter*, (Fall 1995).

Owens William A., 'The Emerging System of Systems', *Military Review*, Vol. 75, No 3, (May-June 1995), 15-19.

Starr B., 'Russian bomb-disarming device triggers concerns', *Jane's Defence Weekly*, Vol. 29, No 11, (18 March 1998), 4.

Starr B., 'USA's rapid targeting reaches new heights', *Jane's Defence Weekly*, Vol. 29, No 9, (4 March 1998), 22-23.

Stein G. J., 'Information Warfare', *Air Clues*, (April 1996), 124-129.

Vorob'ev I. N., Maj Gen(Reserve), Doctor of Military Science, 'Lessons of the War in the Persian Gulf', *VM4-5/(1992),* 64-74.