The

THIRD ELEMENT

A UK Perspective on Information Warfare

Information Warfare is in vogue with militaries in the West. We are, according to the debate, in the midst of a Revolution in Military Affairs (RMA) that sees the Information Age as a Third Wave paradigm shift.[1] Whilst much has been written in the US in an ever increasing deluge, bordering on paranoia, little has emerged from the UK. Notwithstanding the existence of an RMA or, as many believe, a Military Technical Revolution,[2] the issues revolve around how information is treated, its place in operations, its accuracy, expediency and distribution. Much comment has concentrated on the technology itself when, in fact, this is only part of the story. Technology, like any other tool, is useless without the skilled handling by the individual and the organization – a third element is missing.

Abundant and widespread information networks have been driven by systems people without a clear requirement from the operators. It is no surprise therefore that vulnerabilities are rapidly growing, given the lead of technology over business need. This trend must be reversed through the development of doctrine, management and organizational change. In an era of increasingly limited warfare when intolerance of casualties and collateral damage is at an all time high, the time would seem to be right for suggestions for alternative methods of warfighting to be heard by the highest political levels.

It is therefore the intention of this study to offer a British perspective and attempt to shed some light on the way ahead for the UK. By establishing what IW is, why is it becoming so important to defend against it and how it could be adopted as an offensive capability, it is hoped to be able take the debate further. Though this essay will concentrate on the military-strategic level, the reader should recognize that the civilian and military aspects are closely related and in some instances, inseparable. Despite the fact that liberal governments are increasingly sensitive to the use of the word ‘Warfare’ in this subject, I will continue to use the term IW rather than Information Operations – the reader could well treat them as synonymous. I believe IW reflects more of the military aspects of the subject – to examine the whole of Information Operations would demand analysis of government, corporate and societal activity and would be too wide a scope. This paper proposes that although the Technology and Infrastructure elements of IW are in place, the final, crucial element, Organization & Doctrine, must germinate before IW can be a viable option in contemporary conflict.

WHAT IS INFORMATION WARFARE?

The power of computers in general, and of IW in particular is not well understood by the public or most military or national leaders.[3] It is often useful, therefore, to start an analysis with an attempt at defining the key aspects of the argument. As with many topics, definitions are very much in the eye of the beholder; they vary, sometimes, towards the opposite extremes. In desperation, authoritative sources are quoted; these typically include dictionaries or endorsed papers. IW is no exception and is probably one of the more difficult definitions to capture. Many variations of the definition of IW exist and much time has been spent searching for agreement. Pinning down a concept through definition is predominant in the military. Doctrine manuals are becoming widespread and lead off in a mantra that students are expected to learn, parrot fashion, in order to progress and gain understanding. A definition shared by both NATO and the UK, IW is quoted in US Joint Doctrine for Info Operations, JP3.13, as being:

> Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries,

having previously defined Information Operations as:

> actions taken to affect adversary information and information systems, while defending one's own information and information systems.

A variation from US Air Force Doctrine expands further:

> Information Operations (IO) – Those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare (IinW) and information warfare (IW) and are conducted throughout all phases of an operation and across the range of military operations.[4]

Specific UK definitions, whilst agreed between the MOD and the Cabinet Office, have not yet been published. British Defence Doctrine, Joint Warfare Publication 0-01, currently being rewritten by the recently formed Joint Doctrine and Concepts Centre, makes only a passing reference to IW, stating that 'the objective should be to achieve information dominance over the opponent'.[5] These definitions imply that Information Operations are conducted all the time and apply to a far wider audience than just the military. Was Rupert Murdoch's intervention to prevent Harper Collins from publishing Chris Patten's book, heavily critical of the Chinese, a denial of information that would fall under Information Operations? Murdoch was accused of

Murdoch was accused of altering the content of News Corp ventures to avoid offending the Chinese government and thus protect his business interests in China

altering the content of News Corp ventures to avoid offending the Chinese government and thus protect his business interests in China.[6]

Rathmell suggests that IW can be broken into three classes: Category I-new techniques applied to traditional activities; Category II-old techniques applied to new activities and Category III-new techniques applied to new activities – this last category being the most demanding.[7] Schwartau defines IW, using a similar trinity of classes, under the headings Personal, Corporate and Global,[8] each an incremental increase on the previous with effects only varying by degrees of scale. In contrast, Arquilla and Ronfeldt, offer a distinction between what they call "Netwar", a societal-level, ideational conflict waged in part through internetted modes of communication and "Cyberwar" at the military level. Cyberwar may be to the twenty-first century what *blitzkrieg* was to the twentieth. Whereas Cyberwar refers to knowledge-related conflict at the military level, Netwar applies to societal struggles most often associated with low intensity conflict by non-state actors, such as terrorists, drug cartels, or black market proliferators of weapons of mass destruction.[9]

Whilst definitions are a useful area for the protagonists and specialists to debate, there is a danger of spending too much time over nomenclature when more effort placed in evangelism and understanding the issue, its consequences and possible solutions would reap greater benefit. The new concept, struggling to emerge, is the use or targeting of information itself, as a battle winning opportunity, or threat, depending on your perspective. Arquilla and Ronfeldt, moving on from their earlier theses of Cyberwar and Netwar, propose that information has begun to acquire new meanings and imply new possibilities, beyond the dictionary definitions. Closer examination, they suggest, reveals two widespread definitions of information, first as a message and second in terms of a medium. A third more esoteric definition proposes information to be a physical entity, similar to mass and energy. The first proposal is the one that sits most comfortably with the majority of stakeholders. It suggests that information lies in a pyramidal hierarchy that has a broad base of disorganized raw 'data' and 'facts', atop which sits a layer of organized 'information'. The next, smaller stratum relates to a refinement into 'knowledge' and finally, at the peak resides the ultimate 'wisdom' (understanding).[10]

The new concept, struggling to emerge, is the use or targeting of information itself, as a battle winning opportunity, or threat, depending on your perspective

If IW is Information Operations focused in time, space and context then a clearer understanding emerges. IW is not the bailiwick of the military alone - the recent Strategic Defence Review recognised that 'The threat to information infrastructures is not just a defence issue'.[11] A later essay states that under Military Task 26: Military Home Defence, the Government has an obligation to ensure the

…the Government has an obligation to ensure the provision of critical services and the functioning of government itself during times of crisis and conflict. This is achieved primarily by the protection of critical installations and information systems

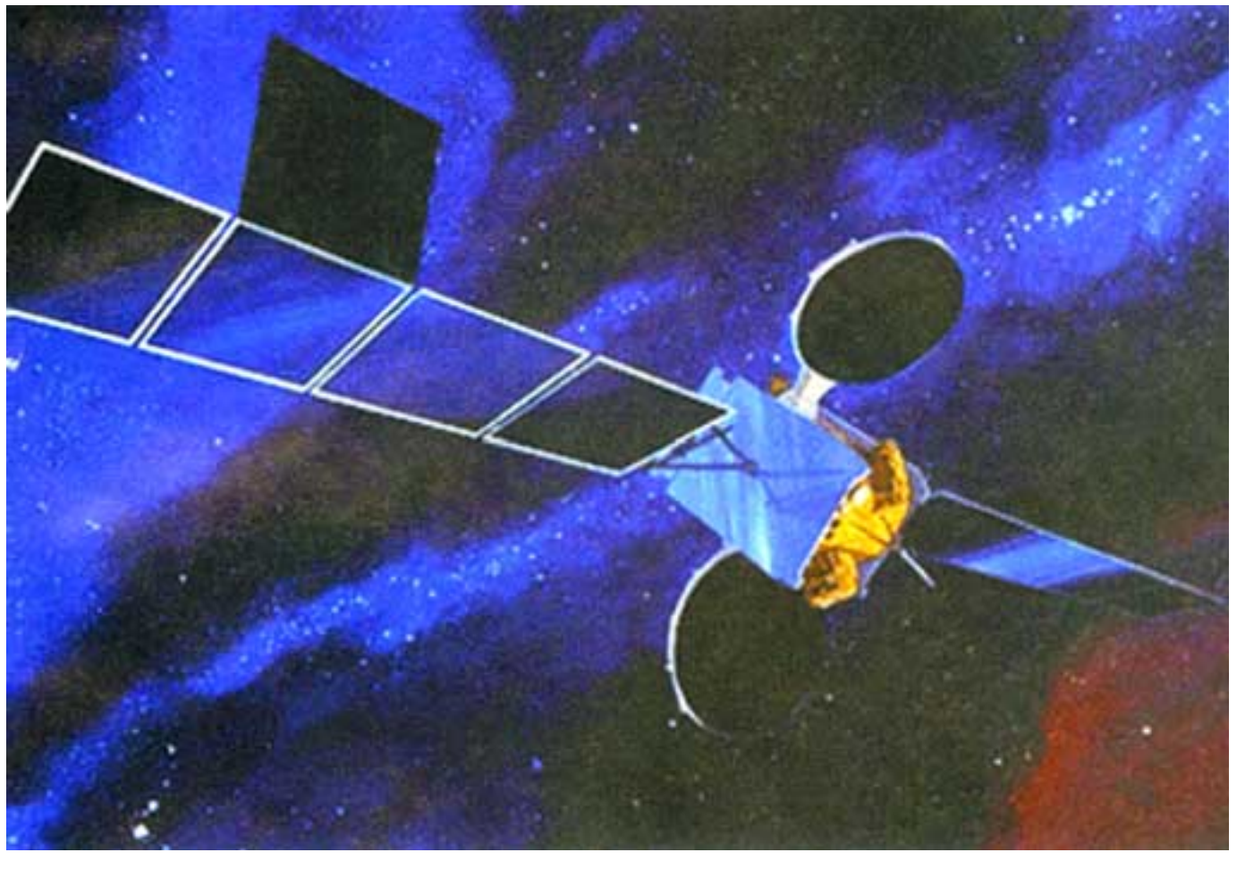
provision of critical services and the functioning of government itself during times of crisis and conflict. This is achieved primarily by the protection of critical installations and information systems.[12] It is unfortunate that the essay goes no further as such a statement covers a whole range of possible responsibilities. The first task must therefore be to establish how vulnerable the military and the Critical National Infrastructure (CNI) really are, in the same way that the US President's Commission on Critical Infrastructure Protection was formed under the Department of Justice to review the US National Information Infrastructure.

An information system could be a telephone network, a predominantly civilian infrastructure that has high value to both military and civilian alike. It is estimated that over 95 per cent of all US military traffic passes over the civilian telephone system – a similar reliance exists in the UK. The CNI is as vital to the military as it is to the population it serves. Indeed, with a continuing drive to shed military roles to 'private partners', this reliance on the CNI is set to increase. The UK Government, after a slow start, is waking up to the implications of IW, acknowledging that 'our dependence on information technology is such that it takes no genius to appreciate that not only enormous benefits but also massive new potential vulnerabilities have thereby been introduced'.[13] Emerging UK policy aims to enable 'both the public and private sectors to operate in an environment which has been shaped in such a way that would-be attackers are deterred and international commerce continues to be attracted to operating with the UK'.[14]

It is also useful to look at what IW isn't – Information *in* warfare (IinW).

> Information-in-war involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated

…were an adversary to deny access to or exploitation of the GPS network, then navigational and weapon strike accuracy might be degraded, but not to the point where offensive operations couldn't be continued



> intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and dissemination activities; and its global navigation and positioning; weather; and communications capabilities.[15]

For example, were an adversary to deny access to or exploitation of the GPS network, then navigational and weapon strike accuracy might be degraded, but not to the point where offensive operations couldn't be continued.

Many observers state that IW is nothing new, that it has been going on for centuries. Well, perhaps this is true but perhaps there is a degree of confusion with what is more accurately labelled IinW. It is a truism to say that information, data, intelligence, call it what you will, is a fundamental ingredient of any major activity. 'Know your enemy…' and other aphoristic cuttings from Sun Tzu are useful educational tools but fail to really shed any light on IW. It has always been the aim of a military operation to deny the opposing commander the ability to command and control his forces. Called (unsurprisingly) Command and Control Warfare (C2W), this strand of warfare is not a thing in its own right but a means to an end. If you are able to successfully win the 'C2W battle' the war is not over – you still have to defeat the fielded forces and, more often than not, induce a territorial shift by physically discharging the 'unlawful' occupants of a disputed region or area. C2W or in its latest guise, IW, can never replace conventional warfare, however limited that becomes. As Brigadier General Marshall wrote:

> Once the total contest between societies is predicated, it becomes impossible to write off the ultimate clash between the masses of men who fight on foot. They are the body of national defence…There is no other way out. The society which looks for an easier way is building its hopes on sand.[16]

The Gulf War has been heralded by many observers as the first Information War.[17] Military firepower was overwhelming on the US order of battle alone, never mind the addition of the coalition assets. Indeed, the coalition and the US in particular, employed and relied upon the latest technology which, coupled with an organizational and training advantage, gave a clear edge over the Iraqi forces. Caution was ever present during the planning and build up to the

The Gulf War has been heralded by many observers as the first Information War. Military firepower was overwhelming on the US order of battle alone, never mind the addition of the coalition assets

coalition offensive. With the ghost of Vietnam in the forefront of all thinking, numbers were increased on more than one occasion to ensure that, when battle was drawn, the allies would have the upper hand. But this, I suggest, was the one and only showing of the classical 'Cold-War Machine' and was Information *in* Warfare taken to its most developed form. Information was essential to the conduct of operations but those operations were conventional counter-force, not counter-information. Although a distinct and developed psychological operations campaign was successfully executed, critical to the subsequent land phase of the conflict, little opportunity either existed, was recognized or was sanctioned for the coalition to strike at the information heart of the Iraqis. Moreover, the conditions for the Gulf War, like so many others, were unique. As a third-class Soviet clone, Iraq was a perfect enemy that particularly suited the US led manoeuvre warfare;[18] it was a unique and distinct coalition of regional protagonists and the sole effective World super power. The techniques and tactics employed exploited technology wherever possible but were successful largely because of superior organization and operational art. However, information failures occurred: as the US Navy's communications systems were largely incompatible with those of the predominant USAF, the Air Tasking Order had to be flown to the ships daily by helicopter. Delays often reduced the planning time available to co-ordinate RAF and US Navy combined missions.[19] The attritional stance adopted by the Iraqis was, from their perspective, the way to win the war – US citizens receiving a blow by blow account on CNN would soon capitulate when the body bags began to pile up. Yet, it became clear to any potential adversary to the US that the asymmetry between conventional forces is likely to be so great that, if conflict arises, an adversary must look for other ways to inflict pain on the World's current superpower – IW could be one such way.

…Iraq was a perfect enemy that particularly suited the US led manoeuvre warfare; it was a unique and distinct coalition of regional protagonists and the sole effective World super power

…if conflict arises, an adversary must look for other ways to inflict pain on the World's current superpower – IW could be one such way

IW consists of a triumvirate of Technology, Infrastructure and Organization & Doctrine. The technology matures at an incredible rate, and according to Gordon Moore of Intel, the number of transistors on a chip of a given size doubles every 18 months. This 'Moore's law' means that the amount of computing power available at a given price also doubles every 18 months.[20] No sooner has a new discovery or manufacturing technique emerged, a step change follows in the performance/cost ratio. What was good yesterday is now woefully inadequate as the continual hardware growth has done little to encourage software writers to develop their skills. So called 'Bloatware' gives rise to excessive code that is error-prone, part undocumented and susceptible to software interference (viruses, etc).[21]

The Internet, a ‘straight research project without a specific application’,[22] born out of a DoD initiative called ARPANet, has grown at an equally alarming rate and in doing so, provides an infrastructure that is not only global in nature but also largely uncontrolled. As the ‘Wild West of cyberspace’,[23] no one owns the Internet and rules and standards, despite the efforts of those who would want to control even a piece of it, are decided upon by the mass of users and a handful of technical specialists.

What is missing or at least is the most poorly developed is the Third Element – organizational change and an underpinning doctrine. Unfortunately, this Third Element of IW has the longest gestation period. Policy and doctrine take months, sometimes years to co-ordinate and agree not only between national actors but also between friends and allies. For this reason alone, it is time to move on to try and close the gap between vulnerability and capability.

WHY WILL IT BE SO IMPORTANT?

Defensive Imperative

With the well established doctrine of overwhelming conventional military force driven primarily by the US but aspired to by the West, a perpetual state of asymmetry exists between future coalitions (including the US) and global adversaries – with the exception of China. The only way for a foe to fight back, on equal terms, would appear to be through terrorist and other exploitable differences. The vulnerabilities, being recognized in a dawn of new understanding, are in Information Technology, Information Systems and electronically stored data.

It understandably worries the US that of all PhD degrees awarded in computer security by US universities, 60 per cent went to citizens of Islamic or Hindu countries

Arguably initiated by the Gulf War and the Toffler study *War and Anti-War,* the US, not surprisingly, are taking a proactive lead. In an ever-tightening process of federal funding, successful programmes have tended to include some aspect or other of IW. It understandably worries the US that of all PhD degrees awarded in computer security by US universities, 60 per cent went to citizens of Islamic or Hindu countries.[24]

Actual attacks like the Solar Sunrise incident or the DoD sponsored exercise, Eligible Receiver have done much to highlight the vulnerability that the US faces, both in the military and in civilian spheres. Eligible Receiver caused quite a stir, bordering on hysteria. Journalists such as James Adams proclaimed that ‘the exercise showed that an electronic Pearl Harbour is not only possible today, it could be completely successful.’[25] However, Adams’ postulations and theories have not always been met with acceptance. Indeed, many criticised his work, The Next World War, for passing on myths and April Fool's jokes, such as the Gulf War virus hoax, as fact.[26] This highlights a problem faced by the US in that the excitable who write on the subject often go

…an electronic Pearl Harbour is not only possible today, it could be completely successful

over the top, inducing an unhelpful paranoia and thus precipitating a serious risk of misdiagnosis. Other doomsday scenarios of total failure of the telephone network, attacks on the New York Stock Exchange, random crediting and debiting from automated teller machines and denial of air traffic control services are commonplace.[27] Clearly a happy medium exists between wild exaggeration and uneducated dismissal. What is unsettling for the US in the case of Eligible Receiver, is that the vulnerabilities exposed by the exercise were known about with fixes suggested – only a few units had bothered to implement them.

High Energy Radio Frequency (HERF) weapons were the subject of a sworn testimony given by Lt Gen Robert Schweitzer before the House Joint Economic Committee, US Congress. In his verbal and written submission, Schweitzer made it quite clear that RF weapons posed a considerable threat to not only military systems, but perhaps more disturbingly, the civilian infrastructure. An attack on Wall Street's computers could be executed through knowledge and equipment available from the Internet and from retail outlets at a cost of a few hundred dollars. Whilst a lot of the scare mongering in the US has the traditional inter-Service battle for federal funding at the heart, not all should be dismissed lightly. In the UK, British Aerospace takes the threat posed by high-energy weapons equally seriously. Such devices are so cheap to build, easy to deploy and conceal and difficult to detect as the source of massive computer failure that they are sure to be high on the list of desirables of any half-competent terrorist organization.[28]

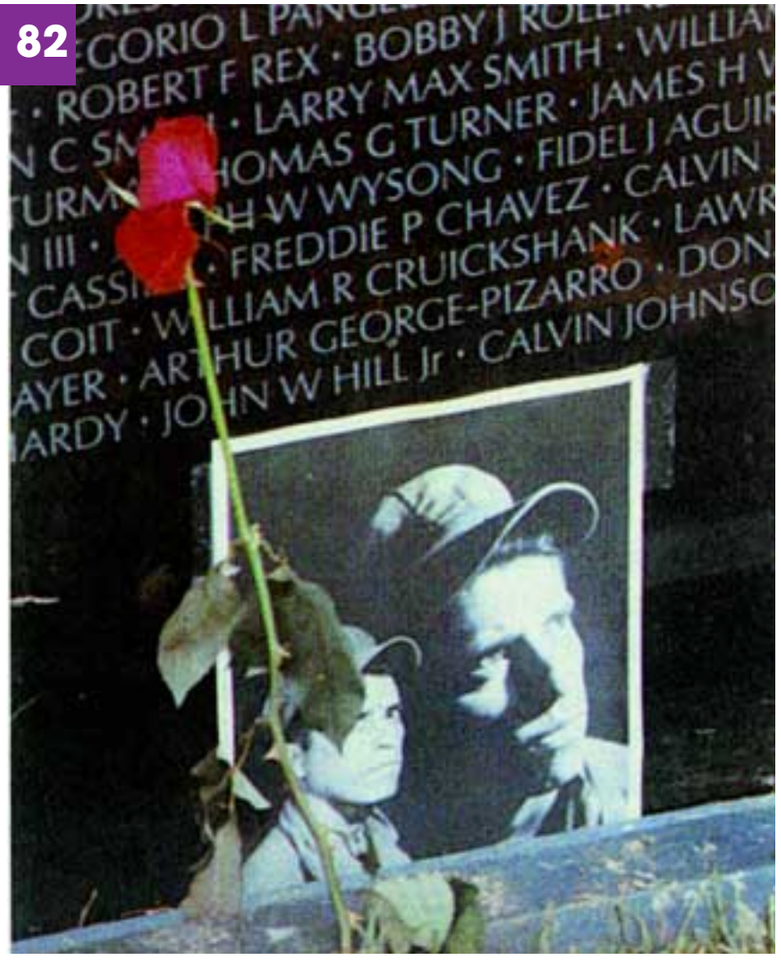
…British Aerospace takes the threat posed by high-energy weapons equally seriously. Such devices are so cheap to build, easy to deploy and conceal and difficult to detect as the source of massive computer failure that they are sure to be high on the list of desirables of any half-competent terrorist organization

In the New World Order that has replaced the bipolar Cold War, risk has a greater emphasis in strategic planning. The pressure on the public purse to take the so-called peace dividend has proved irresistible – now the only way to make the books balance is to increase the emphasis on risk. Such ventures into risk management, hitherto alien business speak, have revealed the need to trust Commercial Off The Shelf (COTS) products to perform critical tasks at critical times. The drawback to huge R&D savings realized by the abandonment of bespoke software, is the risk of at best, bugs and at worst, Trojans or logic bombs that lie dormant, waiting for an activation signal or event.[29] Microsoft Office, used by the vast majority of businesses and militaries the World over, demonstrates the ease at which Trojans can be incorporated. So-called 'Easter Eggs' are software coders 'bit of fun' to demonstrate both coding proficiency and uncontrolled power. By following a series of keystrokes in Microsoft Excel 97, the program executes an audio-visual routine that is completely unrelated to the original purpose of the software – this popular and much praised spreadsheet program contains a fully functional flight simulator.[30] Although benign in the case of Excel, the implications for militaries that depend on COTS software for mission critical tasks are clear.

This dependence on the likes of Microsoft is going to increase and signals a distinct loss of control by the military. Moreover, that an increasing amount of software is now written in India in a collaborative California/Bangalore 24-hour, non-stop cycle, will only proffer further opportunity by non-western, culturally diverse software engineers to introduce 'extras'.[31] Even with control over your supplier in traditional procurement arrangements like those in place for Eurofighter, the fact that software programs increasingly run to millions of lines of code means that it is virtually impossible to fully error check a program before it is introduced to service.[32]

The risk increases as modern, next generation weapon systems such as Storm Shadow are introduced. A long range, stand-off missile, Storm Shadow relies on accurate target data and navigation information to successfully home to the target. Without a man-in-the-loop, it is particularly vulnerable to misinformation and seduction. With a continuing trend to push the man back in the loop, away from the target area, effort must be placed into defensive and protective measures to ensure that such lone weapons reach their target.

In what Luttwak called the paradoxical logic of strategy,[33] each advantage that the West gains from the use of networked information systems brings a home disadvantage and potential opportunity for the adversary. Greater integration of information systems has major benefits, but it also introduces new risks and offers new opportunities for an adversary to attack our information networks, thus degrading the fighting effectiveness of our forces.[34] The more 'wired' a country is, the more vulnerable it is to this sort of [Cyberwar] attack.[35] The asymmetry arising from considerable conventional force, reliance on information systems and uncoordinated defence leaves the UK unnecessarily open to alternative means of attack. If nothing else is done, this threat to the flanks must be addressed.



The seeds were sown for an irreversible change to the face of warfare after the US experience in Vietnam. No longer would Western society put up with high losses and casualties

Offensive Potential

The seeds were sown for an irreversible change to the face of warfare after the US experience in Vietnam. No longer would Western society put up with high losses and casualties. This was a limited war and limits were expected by the distant American people. Such was the pressure of public opinion that political leaders got involved in military planning details of such low magnitude that further damage was done in this first media war. The principle that 'for the moment, war is more a matter of choice than of fait accompli was clearly established – a sea change had occurred.[36]

In 1991, The Gulf War became an information war, not as I have suggested earlier in the way in which it was conducted, but it the way in which it was watched, analyzed, assessed and influenced by a global population.

More information was flowing over the media networks to a World which watched the proceedings in near real-time, from the comfort of an armchair, than had every happened before. Every decision, execution plan and subsequent operation was analyzed by closet experts, hired by the broadcast and print media and consumed by an ever-hungry general public. Here the OODA loop was being spun in the presence of the masses who, on the basis of sound-bites and context-free clippings, exerted considerable influence on the political decision makers.[37] The Al Basra 'Highway of Death', emotively labelled and exposed on prime-time TV, led to Bush calling a halt to hostilities and quashed any additional thoughts of pursuing Saddam to Baghdad. As Michael Evans, Defence Correspondent to The Times said, 'all wars have been completely transformed, whether they be peacekeeping [operations] or high intensity wars, by the presence of the camera'.[38] Indeed, a new form of statesmanship exists which depends less on the individual qualities of our leaders and more on the skill of their spin-doctors and their ability to manage the perception of the people. This creates a second

…'all wars have been completely transformed, whether they be peacekeeping [operations] or high intensity wars, by the presence of the camera'

battlefield where the media and the ‘management’ strive to get their message across. The grisly, real time reporting of the World’s atrocities force the ‘must do something’ reaction that has become so prevalent in Western foreign policy. The strength of the images on our television sets can swing previously resolute governments into taking action that they would otherwise have avoided. Eighteen dead Marines in Somalia in 1994 did more to change US foreign policy than any other single issue – the vivid and disturbing images of a marine being dragged through the streets still haunt both civilian and politician alike.[39] Imagine the consequences, had the BBC been on the ground during the bombing of Dresden in World War II.[40] The insatiable public feed off the images they see, taking without the question the selected edits presented on the ‘box that never lies’. Do something about it but don’t send our boys home in bags.

The insatiable public feed off the images they see, taking without the question the selected edits presented on the ‘box that never lies’. Do something about it but don’t send our boys home in bags

But the classical point is so often missed – war is dangerous. It is not a pleasant activity that occurs between 6 and 9pm for the benefit of the World’s viewers. It is a life and death struggle based on ideology, religion, hatred and oppression and, as such, has few boundaries for those directly involved. When people fight for their very existence, they will do so to the death. The West doesn’t like it. So when calls to intervene are eventually accepted, when the pressure to ‘do something’ reaches that critical point, the basis of international law and sovereignty are ignored and a force goes in to sort it out. But in doing so, it is imperative that only the military targets, as identified, are the subject of attack. *Ius in Bello*, how force is used in war, is paramount for those who believe they are morally just. Any accidental attacks on the civilian populace will not be tolerated, nor will damage to their physical surroundings be accepted: a particularly tall order as the

…opposition, present and future, are learning quickly that high value items should be located near religious artefacts, hospitals and schools. This is a far cry from the accepted attitudes of the total war era – in 1917 Churchill wrote: 'Any injury which comes to the civil population from the process of attack must be regarded as incidental and inevitable'

opposition, present and future, are learning quickly that high value items should be located near religious artefacts, hospitals and schools. This is a far cry from the accepted attitudes of the total war era – in 1917 Churchill wrote: 'Any injury which comes to the civil population from the process of attack must be regarded as incidental and inevitable.'[41]

Minimising collateral damage has also been a high priority but is now a prime concern within western militaries for different reasons.[42] The low tolerance of collateral damage accepted by politicians is based on the reaction of the population to what is seen through the global media. International law rightly demands that non-combatants are excluded and protected as much as possible from the effects of military operations. Collateral damage, from a purist military perspective, is undesirable because of the waste of valuable resources and the resultant need to repeat an attack or operation. If your weapons miss the objective and hit a civilian object, by implication, the military target will need to be attacked again – an inefficient use of resources and an unnecessary risk to those personnel who must repeat the mission. So for more than one reason, there is tremendous pressure to not only hit the correct military target, but also to avoid, at considerable effort, the risk of accidentally striking civilian objects. Add to this memories rekindled of Vietnam and of continual 'hindsight-analysis', generally out of context, of actions that took place in the Second and First World Wars and you have a robust and enduring intolerance of casualties and collateral damage. That said, there is a fair amount of moral fatigue to contend with – so often is the population exposed to disturbing images that perhaps it is becoming *blasé* and more willing to accept the devaluation of life as a sign of the times.[43] Luttwak's logic appears once more: the military's desire to show clinical, precision strikes on TV is based on a need to demonstrate that the rules of war are being rigidly applied. Unfortunately, this gives the inexperienced viewer the impression that every attack will 'go down the air conditioning shaft' – when weapons go awry, the impact is that much more significant and the intolerance escalates. The military is then further constrained with the weapons it may employ to achieve the aim.

The temptation to use IW techniques will be more and more compelling as the global tolerance of collateral damage continues to reduce. The desire for zero casualties will continue to drive research into Non-lethal Weapons (NLW) that 'disable and contain rather than kill and pose minimum long term harm, either to combatants or to the environment'.[44] IW is a logical corollary to this trend, assuming that IW techniques, totally or in part, can be considered non-lethal use of force. The default, "fail-safe" position would seem to be to treat information operations as if they were in fact a use of force.[45] As Barnett continues, 'if the case can be made and sustained that particular forms of information operations do not constitute uses of force, they could be very valuable assets for national security.The debates over IW, Category III in particular, being a non-lethal use of force, if a force at all, have yet to be entered in earnest, given the relatively recent acceptance that IW must be taken seriously. Article 42 of the

UN Charter is concerned with the use of force whereas Article 41 deals with measures not involving the use of force (ie sanctions).[46] Which Article to apply to an IW attack would clearly be an area for significant further work. Indeed, William Church advocates that the next logical step is a comprehensive review of IO weapons and tactics that places them in context of Protocol 1 to the Geneva Convention.[47] However, it may be that the reactionary nature of International Law means that nothing will be done until a serious attack has taken place:

> Chief Justice Oliver Wendell Holmes once wrote, "The life of the law has not been logic; it has been experience." It seldom happens that a legislature foresees a problem before it arises and puts into place a legislative solution before it is needed. More typically, legislators react to a problem that has already manifested itself. The international legal system operates in the same manner.[48]

There is also a battlefield shift in what are commonly called Peace Support Operations (PSO) or Military operations other than War (MOOTW), military activities below the threshold of conventional war. No longer are battles conducted away from the population in defined arenas that are largely free of non-combatants. Warfare, limited though it is, is increasingly conducted in urban environments. Not only is this highly dangerous to the attacking, 'peace-enforcing' force, it is completely unsuitable for the weapon systems that make up a traditional fighting unit. Heavy armour, unguided bombs and missiles can not be effectively employed in urban areas without causing considerable collateral damage. Thus the considerable emphasis placed on urban warfare in the twenty-first century, highlighted by the US Marine Corps' *Sea Dragon* programme to develop new forms of expeditionary warfare.[49]

The most benign act, in total war context, can resolve or induce a perception that achieves the strategic aims

If interpretations of International Law shape and influence conventional operations, it can be seen that attacks of tactical targets with tactical platforms can have strategic and grand strategic impact, dependent on the conditions at the time. Thus we are in an era of perception management where the targeting process is refocused on achieving strategic effect. The most benign act, in total war context, can resolve or induce a perception that achieves the strategic aims. Perception management therefore offers greater opportunity for alternative applications of force and opens the door for NLW and IW options. However, in considering the use of IW techniques, it is vital to consider the likely response of your adversary. The use of conventional explosive force tends to send a relatively clear message. In the height of crisis management, the induced failure or recognised interference with adversary information systems may have an unpredictable effect on his next move:

> The use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not….considering the possible catastrophic consequences of the use

of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces….Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[50]

IW can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results.[51]

In the coercive operations that typify PSO or MOOTW, the strategic objective is to send a clear and unequivocal message to the adversary. Either the state in question meets the demands of the International Community, generally espoused in the form of a UN resolution, or it will continue to suffer the effects of action, increased in intensity to a point when it has no choice but to accept. This is an important change from Strategic Attack to Strategic Effect. In considering the use of IW techniques, it must be certain that Strategic Effect can be induced. Will the source of the IW attack be obvious to the opponent or will the activity be open to hijack by a third actor? What assurances are there that the planned activity will achieve the desired result? Given the shortfalls and extras that already bug COTS software, what assurances are there, if any, that the particular mixture of hardware and software employed by the adversary will respond in the expected way to the IW damage mechanism employed? Most importantly, how, when considering Battle Damage Assessment, 'essential to provide credible and comprehensive analysis to determine the effectiveness of attacks', will the induced effects be identified?[52] It is hard enough to get an assessment of the damage inflicted with conventional weapons, even with the considerable intelligence collection assets available to the UK. It is therefore likely to be extremely challenging for the British military culture, infatuated with tangible statistics, to measure the strategic effects and consequences of IW.

IW can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results

Precision engagement will be just as important with IW attacks as it is with traditional methods. Just as sanctions are hard to focus, IW campaigns could be difficult to precisely control. Above all in considering the potential for the offensive use of IW, is your adversary's susceptibility. Time after time, conflict after conflict, Western governments and their militaries consider the likely enemy courses of action based on the assumptions and culture inherent in our Western Way of Warfare.[53] The UK, more so the

Unless an adversary depends on interconnected information systems, there is little point attempting to deny or destroy them

US, depends on the creature comforts of capitalism to such a degree that if they were to be interfered with, the results would be significant. Unless an adversary depends on interconnected information systems, there is little point attempting to deny or destroy them.

THE THIRD ELEMENT

There is an unfortunate track record when it comes to technology and its adoption into normal working life. Despite the claims and advice from visionaries, militaries tend to work very hard to adapt new technologies to familiar working practices. A ready acknowledgement of the potential and utility of innovation is often an attempt to avoid revealing the true story – a failure to really understand the implications. For example, in 1870, with their newly developed, rapid firing *mitrailleuse*, the French enjoyed a tremendous potential firepower advantage over the Prussians. Unfortunately, this early version of the machine gun looked more like a field piece instead of a rifle, and it was deployed behind the front with the artillery. Thus, the weapon that would dominate World War I a generation later had almost no effect on the Franco-Prussian conflict.[54] In contrast, DiNardo and Hughes argue that history has also repeatedly shown that technology is best incorporated in the context of enhancing such methods that have already proven successful.[55]

…'information has always been a source of power, but it is now increasingly a source of confusion. In every sphere of modern life, the chronic condition is surfeit of information, poorly integrated or lost somewhere in the system'

More than just technical solutions are needed. 'A focused and coherent technology strategy' [56] will indeed be an essential element but it is not the hardware that is the issue – the Vietnam War proved that high technology does not in itself win wars.[57] Because it is so easy to send information, a bizarre logic is commonly adopted by many users that dictates that everyone must want the information – scattergun or push delivery methods don't solve problems but do clog inboxes and overload users. As Wilensky once put it, 'information has always been a source of power, but it is now increasingly a source of confusion. In every sphere of modern life, the chronic condition is surfeit of information, poorly integrated or lost somewhere in the system.'[58]

The success of the first 2 elements of the IW triumvirate has unfortunately resulted in a swing towards information deluge. Control must be regained (assuming it was there in the first place) and thus a key requirement will be an Information Management Strategy (IMS). Until information is treated as a strategic asset in the same way that conventional forces, combat arms training, readiness and everything else that is critical to operations is treated, IW issues

will continue to be addressed in a muddled and confused, *ad hoc* way. Such an IMS must reach across all elements of government and industry, be all embracing, covering every type and classification of information handled, required or produced by defence.[59] It must emphasize the blurring of traditional boundaries in the levels of warfare, Strategic, Operational and Tactical, and get away from the traditional 'stove-piping' of information into operational and non-operational, formal and informal, classified and unclassified. Information must add value to an individual or group, a period of time during which it holds that value, an owner or sponsor who's task is to ensure that the value remains, otherwise the information must be removed.

Perhaps information itself is not the real issue. A librarian has custody of a large amount of information but cannot, through volume, use that information to create knowledge unless the librarian task is dropped and a more scholarly one adopted. Thinking back to Arquilla and Ronfeldt's pyramid, they suggest that '...an excellent manager with poor information may be able to make some good decisions through intuition; an average manager with quality information will make better decisions consistently' – the key word being quality.[60] A knowledgeable manager may be able to make equally good decisions with variable quality and quantity information whereas a wise manager may not need any information at all. There have been many situations in which commanders had virtually all the information possible on enemy strength and dispositions but could not transform it into an understanding of enemy intentions.[61] Selection and Maintenance of the Aim, the cardinal Principle of War,[62] is hard to achieve when a constant stream of variable quality information can tempt commanders into waiting just a little longer before making a critical decision.

For an IMS will be a stepping stone to a greater goal – knowledge through sharing. Campen tacitly avers the truth, suggested by Sun Tzu 2,500 years ago, that the ultimate goal of the struggle is to dominate the enemy in knowledge, not information. Collection and analysis of information is, of course, a part, but not the whole.[63] By looking after a key ingredient to knowledge, information can be collected, used, disseminated and interpreted to create something that adds value to the core output task of the organization. Collection has never been a problem, indeed it is one of the UK's strong points – whether the most is gained from that collected information is more doubtful. The orchestration of this process revolves around the adoption of information management as a core responsibility of those in the command chain. At every level, information needs are different and focused to the task in hand. It is suggested that the *baton* be held by a Chief Information Officer who would help lead and direct the organization by ensuring that information is treated strategically. Whilst Art Money, the US Assistant Secretary of Defence for command, control and communications has recently been appointed CIO in the US, such a post has yet to be filled in the UK.

Organzational changes will be harder to adopt. A natural and compulsive hierarchy, the military needs to reap the benefits of networking without losing the structure of the Command Chain, so important to the conduct of military operations in an increasingly complicated and difficult strategic environment. The Joint Battlespace Digitization programme suggests concepts of

an information equipped soldier having data-link, real time updates and control – such potential must be treated carefully. It would be unwise to vest the decision-making material of the military with such a low denominator. Indeed, as Sullivan warns:

> Junior infantry…may be connected electronically to sources of awesome firepower….Privates or lance corporals might control more destructive power than an entire army corps possessed in World War II. But would it be wise to entrust such capabilities to nineteen- or twenty-year-olds, however intelligent, well-trained and psychologically stable?[64]

On the other hand, the trend for micro-management through a growing desire for commanders to be in the cockpit or at the head of the platoon must be reversed. So-called 'forward leadership from the rear',[65] four-star generals, senior civil servants and even prime ministers make poor combat pilots or soldiers.[66] Unfortunately, history is full of examples of this disruption of the command chain, the most memorable being Lyndon Johnson essentially conducting the defence of Khe Sanh from a sand table in the White House.[67]

Networking offers many opportunities for redundancy as many alternate paths exist to information or decision. Such a concept would be unworkable in its own right within traditional military circles. Yet the hierarchy that must exist between the electronic protagonists of government and commerce will strain towards such a solution. What will be key for the military is for it to decide where it can comfortably operate between the opposites of networked organization and organizational networks.

Of prime importance is the way in which the organizational culture change is introduced with the people who interact with the system of systems. For many personnel, military and civilian alike, the concepts surrounding IW are both alien and abstract. Many have grown up outside of the information age in a time when computers where physically enormous, occupying separate departments of large corporations and whose operators spoke another language. Whilst some would say the latter is still true, many find themselves at the command of far more power in a much smaller form resulting in fear, distrust and frustration. To many users, it isn't as 'obvious', as the help desk suggest or as their children demonstrate.

Given that connectivity, when it arrives, will bring a new, greater vulnerability to the UK, it is imperative that defensive mechanisms are put in place as a matter of priority. Defence in Depth must be a principle to adopt. Combinations of physical, technical and procedural security will be needed to build up a robust information assurance core to the collective whole. Probing and testing by 'Red Teams' and 'CERTS' will be fundamental to any strategy that seeks to exploit and defend against the possibilities and disadvantages of this revolution.[68] Such Information Assurance mechanisms must not 'play the blame game' [69] but must offer constructive criticism and practical remedies – to do otherwise would be to create a 'PC police' image that would impair the culture change process.

The number of users whose password is 'password' is so widespread that system designers must now start to think like system users and develop passive systems such as biometrics for user identification

One of the greatest physical risks to security stems from human nature. Used properly, passwords are a robust mechanism to ensure that access to information systems is restricted to those that need it. If you can remember a mixture of alphanumerics and characters in upper and lower case and then learn a new 'word' every couple of months then all is well. Unfortunately, the average user, left to his or her own devices, will select something a little more memorable, but often predictable. The number of users whose password is 'password' is so widespread that system designers must now start to think like system users and develop passive systems such as biometrics for user identification.

Technical contributors to defensive IW (Information Assurance in emerging UK doctrine [70]) include artificial intelligence, neural learning systems such as the IW Attack Assessment System (IWASS) which can be used to evaluate potential threats, provide Indicators and warnings of an IW attack and to predict likely courses of action.[71] Other network software tools are available to monitor proceedings and to look for the unusual. It must be remembered though, that detecting attack will be an increasing part of the training that must be given to users of all levels and variations of military information systems. Detection will be an issue. Screens will not go blank – the data displayed will be subtly manipulated making what is seen plausible but wrong. This interference is all the easier now that, for example, raw radar displays have been replaced by computer generated situation displays, in convincing colour and clarity. Those hard-won skills that, through experience and training, enabled operators to work through electronic interference, are fading fast. Many have become system operators who no longer need the skill of a craftsman to get the required output.

According to an Organisation for Economic Co-operation and Development research paper, *Technology upgrading with Learning Cost – A Solution for Two Productivity Puzzles*, by Sanghoon Ahn, productivity declines initially when technology is introduced because people take time to learn how to use it. Later, however, benefits show through. What happens though, when the rate of change of technology is so great that you never get beyond the downward learning phase and into the upward productive phase?[72] Less of Moore and more of Ahn would enhance capability by ensuring that users can fully exploit opportunity and effectively resist sabotage.

As far as offensive opportunities are concerned, the systems approach to targeting that has been developed on both sides of the Atlantic since the Gulf War will need to be expanded and refined. If IW techniques, including Computer Network Attack are to be developed and introduced into the repertoire of potential responses, then an intelligence cost can be expected. Whereas the crew of an aircraft dropping an iron bomb can manage to complete the task with rudimentary intelligence, to expect the same of an IW based attack is to court failure. The level of detail that will be required to successfully interfere electronically will

Whereas the crew of an aircraft dropping an iron bomb can manage to complete the task with rudimentary intelligence, to expect the same of an IW based attack is to court failure

be significant. But systems analysis pays off and, if approached methodically, is generally worth the effort expended. Every [target] system has its weakness, its Achilles Heel. Whether to use conventional force or IW/IO against this weakness will depend on the situation at the time. That the two options should be closely co-ordinated cannot be overstated.

CONCLUDING THOUGHTS

History gives us no clear definition of what constitutes an RMA but emphasises that an RMA is not a precise phenomenon that has a clear start and end point or indeed, can be recognised as happening without the need for historical analysis.[73] So has there been a Revolution in Military Affairs? As yet, the sort of dramatic shift that typified the industrial revolution has just not materialized. There is certainly rapid change but this is much more evolutionary in nature. The biggest change in the conduct of future military operations is likely to come not from the weapons alone but from the application of information technology to military command and control.

The biggest change in the conduct of future military operations is likely to come not from the weapons alone but from the application of information technology to military command and control

The Third Element must be developed to bring together Technology and Infrastructure in an orchestration of capability. A thorough understanding coupled with willingness for organizational change must be underpinned by a doctrine that illuminates and educates. Government and military must tackle the more intangible Category III IW, from Netwar to Cyberwar. It may be anathema to employ hackers and crackers but it they have a monopoly in the skill set then there appears to be little alternative.

The UK certainly believes that radically improved capabilities in the field of information processing and communications systems will increase situational awareness by combining information from all available sources and rapidly distributing it to those who need it, thus permitting more effective and efficient use of our forces.[74] Smart long-range precision weapons will enable us to attack targets accurately from distance, thereby reducing our own and civilian casualties.[75] But this capability enhancement currently has the hallmarks of a Military Technical Revolution and is not a panacea; it is merely an additional option for use in specific circumstances against an adversary susceptible to its damage mechanisms. Offensive opportunities, sensitive as they are, should be properly resourced and offered up to the political leadership as a potential alternative course of action.

The first element of the triumvirate of IW, information technology, has been evolving since the seventies and the second, the Internet or World Wide Web, once a critical mass of users were attracted, has been growing exponentially. Both have been rapid by any standard but, nevertheless, evolutionary. Journalists and documentary makers across the World extol the wonders of IW, dipping freely into the rich pool of Toffler catch-phrases with remarkably uncritical abandon.[76] But much work remains to be done, both in definitional terms, in international relationships and doctrine, not to mention national issues such as policy lead, requirements and potential impact on the way that the UK Ministry of Defence conducts its business in the arena of IW. If it is to avoid being left behind, the UK must learn from this confusion, sidestep time-wasting at the boundaries and contribute to the debate by offering clarity of thought in 'a holistic assessment of national vulnerabilities' and a measured analysis of the opportunities.[77]

Information can only be an object of warfare when its value, to both sides, is understood. Without a top-level strategy on Information Management, any resulting doctrine and order will be the result of good fortune rather than good planning. If IW is to be another 'club' in the golf bag of statehood, then considerable effort must be put into the development of coherent doctrine – we must learn how to play with this new club. An understanding of the relationship between the Information Age and national security should be high on the agenda of any nation wanting to exploit the offensive opportunities of IW and ensure that it can defend itself against emerging threats. As Libicki suggests, '[US] vulnerability is greater than it ought to be but should not be exaggerated' – while the UK is not yet as exposed, it is only a matter of time. That time should be used to develop a robust and coherent Third Element by learning how to disseminate, protect and exploit information shared between the UK's military, government, industry and the society they all serve. Having achieved such a considerable task, the interoperability issues between NATO and potential coalition partners need to be addressed. If understood correctly, IW would lose its sex appeal or media attention and it would disappear from Presidential Decision Documents and grand national strategy – but it would grow up and go to work.[78] Perhaps then it will be possible for information to be a weapon of war. Moreover, it may take the ascendancy of the information generation to the height of both military and civilian office before the real potential of IW can be realized and a complete culture change enabled. Whether a revolution takes place or not will be up to future historians to debate – the seeds have certainly been sown.

BIBLIOGRAPHY

Adams, James, *The Next World War*, (London: Random House, 1998).

AP3000 British Air Power Doctrine, 3rd edition, (HMSO 1999).

Arquilla and Ronfeldt (eds)., *In Athena's Camp, Preparing for conflict in the modern age,* (Rand. 1997).

Arquilla, J and Ronfeldt, D, *Cyberwar Is Coming!*, International Policy Department, (RAND, Taylor & Francis, 1993).

British Defence Doctrine, JWP 0-01, (London: Caldwell Prince, 1997).

Broughton, J, *Going Downtown: The War against Hanoi and Washington*, (New York: Pocket Books, 1988).

Campen, Alan D., ed., *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War* (Fairfax, Va.: AFCEA International Press, 1992).

Campen, A., Dunnigan, James F. and Bay, Austin, *From Shield to Storm: High-Tech Weapons, Military Strategy, and Coalition Warfare in the Persian Gulf* (New York: William Morrow and Co., 1992).

Campen, A. & Dearth, D., *Cyberwar 2: Myths, Mysteries and Reality* (Fairfax, VA: AFCEA Press, 1998).

Clausewitz, Carl von, *On War*, ed. and trans. Sir Michael Howard and Peter Paret, (Princeton: Princeton University Press, 1984).

Fuller, JFC, *The Conduct of War 1789-1961* (London: Eyre Methuen, 1972).

Garfinkel, Simson and Spafford, Gene, *Practical UNIX and Internet Security*: 2nd Edition, (O'Reilly & Associates, Inc., 1996)

Greengberg, Goodman and Soo Hoo, *Information Warfare and International Law*, (Washington, DC: NDU Press, 1997).

Huntington, Samuel P. *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge, Mass.: Belknap, 1957).

JSP 398, UK Rules of Engagement.

Joint Warfare Publication 0-10, *UK Doctrine for Joint and Multinational Operations*, Ratification Draft Edition 1, 17 August 1999, Crown Copyright.

Khalilzad, Lesser, *Sources of Conflict in 20th century*, (California: Rand, 1998).

Libicki, Martin C. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, (Washington, DC: NDU Press, 1994).

Libicki, Martin C. *What is Information Warfare?* (Washington, DC: NDU Press, 1995).

Luttwak, E N, Strategy: *The Logic of War and Peace*, (Harvard University Press: Cambridge Mass., 1987).

Lynch, Daniel C., 'Historical Evolution,' in *Internet System Handbook*, Daniel C. Lynch, and Marshall T. Rose, eds, (Greenwich, CT: Addison-Wesley Publishing Company, Inc., 1993).

Molander, R., Riddile, A., Wilson, P., *Strategic Information Warfare: A New Face of War* (Washington DC: RAND, 1996).

Munro N, *The Quick and the Dead*, (New York: St Martin's Press, 1991).

Pfaltzgraf, Jr, Robert L, and Shultz, Jr, Richard H, (Eds.), *War in the Information Age: New Challenges for US Security*, (Washington: Brassey's, 1997).

Roszak, Theodore, *The Cult of Information; The Folklore of Computers and the True Art of Thinking*, (Lutterworth, October 1985).

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994).

Scheitzer, James A., *Managing Information Security*, 2nd Ed., (Butterworth: Stoneham, MA, 1990).

Sills, David L. (Ed.), *The International Encyclopedia of the Social Sciences*, Vol. 11, (New York: Macmillan & the Free Press, 1967).

Sun Tzu, *The Art of War*, Translated by Samuel B. Griffith. (New York: Oxford University Press, 1971).

Toffler, A. & Toffler, H., *War and anti-war: Survival at the Dawn of the 21st Century* (Boston: Little, Brown & Co, 1993).

UN Charter.

Van Creveld, Martin, *The Transformation of War* (New York: The Free Press, 1991).

Van Creveld, Martin, *Technology and War: From 2000 B.C. to the Present* (New York: Free Press, 1989).

Warden, Col John A. *The Air Campaign: Planning for Combat* (Washington, D.C.: NDU Press, 1988).

Wilensky, H., 'Organizational Intelligence', in *The International Encyclopedia of the Social Sciences*, David L. Sills (Ed.), Vol. 11, New York: Macmillan & the Free Press, 1967.

Magazines, Periodicals & Journals

Airpower Journal, Spring 1995.

Airpower Journal, Summer 1995.

Defense News, 30 Nov – 6 Dec 1998.

Economist, 13 January 1996.

Economist, 23 March 1996.

Financial Times, 28 Feb 98.

Parameters, Summer 1999.
RAF Air Operations Manual, Second Edition (draft).
RAF Air Power Review, Autumn 1999.
RUSI Journal, February 1996.
RUSI Journal, October 1997.
RUSI Journal, October 1997.
Sunday Times, 22 August 1999.
Strategic Review, Vol 24, No 2.
Washington Times, 16 April 1998.

Other Sources

Arquilla, John. 'The Strategic Implications of Information Dominance' *Strategic Review* 22 (Summer 1994):

Aldrich, Major Richard W., USAF, 'The International Legal Implications of Information Warfare'.

Arthur, Charles and von Herberstein, Nicholas, *Cyberterror Attack Rocks America*, email mailing list, 5 Mar 98.

Bugliarello, Dr George, *Telecommunications, Politics, Economics and National Sovereignty – A new Game*. Presented at the Conference on Communications Technology and National Sovereignty in the Global Economy, 21-22 April 1995, Northwestern University.

Baumard, Philippe, Ph.D. Professor of Strategic Management, University of Paris-XII, *From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift.*

Conduct of the Persian Gulf War: Final Report to Congress, vol. 1 (Washington, D.C.: Department of Defense, 1991).

Cramer, Myron L., *Economic Espionage: An Information Warfare Perspective*.

Czerwinski, Thomas J., The Third Wave: *What the Tofflers Never Told You*, NDU, Institute for National Strategic Studies, April 1996. http://www.ndu.edu/inss/strforum/forum72.html.

Devost, M. G., 'National Security in the Information Age', thesis presented to University of Vermont, May 1995.

Devost, Matthew G., Houghton, Brian K. and Pollard, Neal A., *Information Terrorism: Can You Trust Your Toaster?*

Electronic Business Without Fear: The TriStrata Architecture, a White Paper from Pricewaterhouse Coopers LLP, June 1998.

Evans, Michael, Defence Correspondent to *The Times*, Telephone interview 11 June 1996.

Freedman, Lawrence, 'The Revolution in Strategic Affairs', *Adelphi Paper 318,* April 1998.

Gompert, David C., *Information Warfare: A Two-Edged Sword – Keeping Information Warfare in Perspective*.

Howard, John D., *An Analysis of Security Incidents on the Internet*, Carnegie Mellon University,1989–1995.

Heeks, Dr Richard, Senior Lecturer, Information Systems & Development, Institute for Development Policy & Management, University of Manchester [richard.heeks@man.ac.uk], email interview, 20 Sep 99.

Information Warfare conference proceedings, Royal United Services Institute, 2-3 December 1998.

Information Warfare conference proceedings, SMi 3rd Annual conference, 10-11 March 1999.

Layton, Group Captain P., RAAF, *Network-Centric Warfare: A Place in Our Future?*, Air Power Studies Centre, Fairbairn, 1999.

Libicki, Martin, 'Defending Cyberspace and Other Metaphors', Institute for National Strategic Studies, NDU.

Love, Group Captain D., Deputy Director Security, Communication and Information Systems (RAF). Interview, 7 June 1999, Ministry of Defence, Whitehall.

McCulloch, J, Future Systems Division, British Aerospace, Interview, 24 Sep 99.

Parsons, Capt David Willard, USAF, *British Air Control: A Model For The Application Of Air Power In Low-Intensity Conflict?*

Presidential Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, (Government Printing Office: Washington DC: 1997).

Rathmell, A, *Information Warfare and the Asymmetric Threat: An Approach to Early Warning*.

Rathmell, A, 'Cyber-terrorism: The Shape of Future Conflict?', *RUSI Journal* October 1997, pp. 40-46.

Schweitzer, Lieutenant General Robert L., U.S. Army (Retired), *Radio Frequency Weapons And The Infrastructure*, submitted to the US House Joint Economic Committee on June 17, 1997.

Scorer, Captain S. J., Royal Navy, Directorate of Joint Warfare – Information Operations (Plans). Interview, 14 September 1999, Ministry of Defence, Whitehall.

Sullivan, Brian R, 'Spacepower and America's Future' the planned final chapter of Peter L Hays, ed., *Spacepower for a New Millennium* (Colorado Springs: US Air Force Institute for National Security Studies, forthcoming).

Sommerville, Mary A., ed., *Essays on Strategy XIII* (Washington, D.C.: National Defense Univ. Press, 1996).

'An Assessment of International Legal Issues in Information Operations', May 1999, Department of Defence,

Office of General Counsel, http://www.infowar.com/.

Office of the Undersecretary of *Defense for Acquisition & Technology, Defense*

Science Board Task Force on Information Warfare – Defense Department of Defense, Washington DC, November 1996.

Strategic Defence Review, Supporting Essay Three, 'The Impact Of Technology', July 1998.

Strategic Defence Review, Supporting Essay Six, 'Future Military Capabilities', July 1998.

Web Links

http://www.cfcsc.dnd.ca/
http://www.uta.fi/~ptmakul/infowar/index.html
http://www.rand.org/publications/RRR/RRR.fall95.cyber/
http://www.Canadiantom.com
http://www.fas.org/irp/wwwinfo.html
http://www.psycom.net/iwar.1.html•Student Number 95/A10024
http://www.senate.gov/~levin/comsec.html
http://www.cadre.maxwell.af.mil/warfarestudies/iwac/iwacpage.html
http://www.infowar.com/
http://www.cesg.gov.uk/
http://www.parliament.the-stationery-office.co.uk/pa/cm/cmhansrd.htm
http://www.kcl.ac.uk/orgs/icsa/infowar.htm#infowar
http://www.kcl.ac.uk/orgs/icsa/lar
http://eastereggs.8m.com/eggs/excel.html
http://www.aracnet.com/~gtr/archive/info_war.html
http://www.i-war.com/
http://www.us.net/signal/Infowar/infowar.html
http://mindit.netmind.com
http://www.emergency.com
http://www.ilf.net
http://www.2600.com/hacked_pages/
http://www.canadacomputes.com/tc/Apr97/F-HOAX.html
http://www.rsa.com/rsalabs/pubs/cryptobytes/
http://www.wired.com
http://www.eff.org

NOTES

1 Thomas J. Czerwinski, 'The Third Wave: What the Tofflers Never Told You', NDU, Institute for National Strategic Studies, April 1996.

2 It is not my intention to analyse in depth the existence or otherwise of an RMA, a term developed by Soviet Military Theorists in the period c. 1950-70. For specific works on the subject see: Wing Commander D Caddick, 'The Revolution in Military Affairs – Panacea or Myth?' in *The RAF Air Power Review*, Autumn 1999; Brian R Sullivan, 'Spacepower and America's Future' the planned final chapter of Peter L Hays, ed., *Spacepower for a New Millennium* (Colorado Springs: US Air Force Institute for National Security Studies, forthcoming); P L Ritcheson, 'The Future of Military Affairs – Revolution or Evolution?', *Strategic Review*, Vol 24, No 2 and Lawrence Freedman, 'The Revolution in Strategic Affairs', Adelphi Paper 318, April 1998.

3 Martin Libicki, 'Defending Cyberspace and Other Metaphors', Institute for National Strategic Studies, NDU, http://www.ndu.edu/inss/actpubs/dcom/dcomcont.html.

4 http://www.cadre.maxwell.af.mil/warfarestudies/iwac/define.html.

5 *British Defence Doctrine*, JWP 0-01, (London: Caldwell Prince, 1997), p. 4.13.

6 *Financial Times*, 28 Feb 98.

7 A. Rathmell, 'Cyber-terrorism: The Shape of Future Conflict?', *RUSI Journal,* October 1997, pp. 40-45.

8 Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994).

9 John Arquilla and David Ronfeldt, *Cyberwar Is Coming!*, International Policy Department, (RAND, Taylor & Francis, 1993).

10 Arquilla and Ronfeldt, 'Information, Power and Grand Strategy' *In Athena's Camp* (National Defense Reasearch Instituite, Rand, 1997) pp 144-146. Admiral J W Prueher, Commander in Chief, US Pacific Command, 'Information Age Overload:More Data Does Not Mean Superior Judgement', in *Defense News*, 30 Nov – 6 Dec 1998.

11 *Strategic Defence Review*, Supporting Essay Three, 'The Impact Of Technology', July 1998, http://www.mod.uk/policy/sdr/essconts.htm.

12 *Strategic Defence Review*, Supporting Essay Six, 'Future Military Capabilities', July 1998, http://www.mod.uk/policy/sdr/essconts.htm.

13 David Fisher, Deputy Head of the Defence and Overseas Secretariat, Cabinet Office, in the opening address of an Information Warfare conference held at Royal United Services Institute, 2-3 December 1998.

14 *Ibid*.

15 http://www.cadre.maxwell.af.mil/warfarestudies/iwac/define.html.

16 Brigadier General S L A Marshall, 'Men Against Fire – The Problem of Battle Command In Future War (first published in 1947), (Peter Smith, Gloucester, Ma, 1978) cited in Squadron Leader P Emmett, 'Information Mania – A New Manifestation of Gulf War Syndrome?' *RUSI Journal,* February 1996,

p. 26.

17 Colonel Edward Mann, USAF, 'Desert Storm: The First Information War?', *Airpower Journal*, vol 8 no 4, Winter 94, pp 4-14 and Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War* (Fairfax, Va.: AFCEA International Press, 1992).

18 R L DiNardo and D J Hughes, 'Some Cautionary Thoughts on Information Warfare', *Airpower Journal,* Winter 1995.

19 The author flew on many missions during the Gulf War, typically in packages that included RAF bomber and US Navy fighter aircraft.

20 *Electronic Business Without Fear: The TriStrata Architecture*, a White Paper from PricewaterhouseCoopers LLP, June 1998 .

21 For COTS software containing undocumented code, see http://www.eeggs.com. Bloatware: In a typical program only 40% of code is actually used. Paul Zavidniak, 'Warfare in the Year 2010: Defensive IW for Military Aircraft', conference proceedings of the 3 rd Annual SMI Conference on Information Warfare, London, 10-11 March 1999.

22 Daniel C. Lynch, 'Historical Evolution', in *Internet System Handbook,* Daniel C. Lynch, and Marshall T. Rose, eds, (Addison-Wesley Publishing Company, Inc., Greenwich, CT, 1993), p. 5.

23 Simson Garfinkel and Gene Spafford, *Practical UNIX and Internet Security: Second Edition*, (O'Reilly & Associates, Inc., 1996), p. xiii.

24 Libicki, *Op Cit*.

25 James Adams, *'The Enemy Within: A New Paradigm for Managing Disaster',* speech by CEO UPI, Disaster Forum '98 conference, 29 June 1998.

26 See http://www.canadacomputes.com/tc/Apr97/F-HOAX.html

27 Cyberwars, *The Economist*, 13 January 1996.

28 J McCulloch, Future Systems Division, British Aerospace, Interview, 24 Sep 99.

29 *Trojan horse*: malicious computer code located within a desirable block of code (an application program, operating system software, etc.). To be a Trojan horse, the presence of the code must be unknown and it must perform an act that is not expected by the owner of the system. Lawrence G. Downs, Jr., 'Digital Data Warfare: Using Malicious Computer Code As a Weapon', in Mary A. Sommerville, ed., *Essays on Strategy XIII* (Washington, D.C.: National Defense Univ. Press, 1996), p. 45.

30 (1) Open a blank worksheet in Excel 97. (2) Press F5 and type in the range X97:L97, then click OK. (3) Now press Tab once (this should put you in cell M97). (4) Press Ctrl+Shift while clicking once on the chart wizard button. (5) Use the mouse and mouse buttons to navigate. (6) Exit the screen by pressing Esc.

31 'Software in India. Bangalore bytes', *The Economist*, 23 March 1996 and 'India software exports booming' *Reuters* http://news.cnet.com/news/0-1003-200-325488.html.

32 Eurofighter has some estimated 5 million lines of code. Wing Commander P Willis, Eurofighter staff officer, Ministry of Defence.

33 E N Luttwak, *Strategy: The Logic of War and Peace*, (Harvard University Press: Cambridge Mass., 1987), part 1. p. 207.

34 *Strategic Defence Review*, Supporting Essay Three, 'The Impact Of Technology', July 1998, http://www.mod.uk/policy/sdr/essconts.htm.

35 Cyberwars, *Op Cit*.

36 Freedman, *Op Cit*.

37 Observe, Orientate, Decide, Act. A theory developed by Col John R Boyd, USAF, from briefing slides on 'A Discourse On Winning and Losing', August 1987, Maxwell AFB, Alabama, widely accepted throughout NATO and Western militaries. The operational tempo of any campaign is dependent on the cyclic activities that make up the OODA loop. If you cycle those activities faster than your adversary while slowing him down wherever possible, it will lead to success on the battlefield. *AP3000* British Airpower Doctrine, 3 rd edition, 1999.

38 Telephone interview with Michael Evans, Defence Correspondent to *The Times*, 11 June 1996.

39 An interesting paradox given that these professional soldiers come from a country in which gun-related deaths were last clocked at one every 14 minutes. Wing Commander D Caddick, 'The Revolution in Military Affairs – Panacea or Myth?' in *The RAF Air Power Review*, Autumn 1999, p. 60.

40 Martin Bell, *Search for the Truth*, Radio 4, May 1996.

41 JFC Fuller, *The Conduct of War 1789-1961* (London: Eyre Methuen, 1972), p. 280.

42 Collateral damage defined in *JSP 398, UK Rules of Engagement* as 'Damage to personnel and property adjacent to but not forming part of, an authorized target'.

43 Squadron Leader R M Poole, 'Is it Ever Permissible to Kill Non-combatants?' Unpublished paper, 27 Mar 1996.

44 Chris Morris, Janet Morris, Thomas Baines, 'Weapons of Mass Protection: Nonlethality, Information Warfare and Airpower in the Age of Chaos', *Airpower Journal*, Spring 1995, p.15.

45 Barnett, *Op Cit*.

46 See Greenberg, LT, Goodman, SE, Soo Hoo, KJ, 'Information Warfare and International Law', National Defence University Press at http://www.dodccrp.org/iwilexecutiv.htm; Charter of the United Nations at http://www.un.org/aboutun/charter/chapter7.htm.

47 William Church, 'Information Operations Violates Protocol I', 23 Jun 1999, http://www.infowar.com/io_and_violations_of_protocol_i1.htm.

48 Cited in 'An Assessment of International Legal Issues in Information Operations', May 1999, US Department of Defence, Office of General Counsel, http://www.infowar.com.

49 Freedman, *Op Cit*, p.17.

50 V I Tsymbal, "Kontseptsiya 'Informatsionnoy voiny'" (Concept of Information Warfare), speech given at the Russian-US conference on Evolving Post-Cold War National Security Issues", Moscow, 12-14 September, 1995, p.7 in Timothy L Thomas, 'Deterring Information Warfare: A new strategic Challenge', *Parameters*, 26 (Winter 1996-1997), p. 82.

51 S J Cimbala, 'Nuclear Crisis Management and Information Warfare', *Parameters*, (Summer 1999), p. 125.

52 BDD, *Op Cit*, p. 4.16.

53 Freedman, *Op Cit*, p. 15.

54 Arquilla and Ronfeldt (eds)., In Athena's Camp, Preparing for conflict in the modern age (Rand, 1997), p. 41.

55 DiNardo and Hughes, *Op Cit.*

56 Strategic Defence Review, Supporting Essay Three, 'The Impact Of Technology', July 1998, http://www.mod.uk/policy/sdr/essconts.htm

57 Squadron Leader P Emmett, 'Information Mania – A New Manifestation of Gulf War Syndrome?' RUSI Journal, February 1996, p.20.

58 H. Wilensky, 'Organizational Intelligence', in *The International Encyclopedia of the Social Sciences*, David L. Sills (Ed.), Vol. 11, (New York: Macmillan & the Free Press, 1967), p. 331.

59 Captain S J Scorer, Royal Navy, Directorate of Joint Warfare - Information Operations (Plans). Interview 14 September 1999, Ministry of Defence, Whitehall.

60 James A. Scheitzer, Butterworth, Stoneham, *Managing Information Security*, 2nd Ed., 1990. Pg3.

61 Brian R Sullivan, 'The Future Nature of Conflict: A Critique of "The American Revolution in Military Affairs" in the Era of Jointery' in *Defence Analysis* Vol 14, No 2, 1998, p94.

62 BDD, *Op Cit*, p. A.2.

63 Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War* (Fairfax, Va.: AFCEA International Press, 1992).

64 Sullivan, *Op Cit*, Pg 98.

65 N. Munro *The Quick and the Dead*, (New York: St Martin's Press, 1991), p80.

66 J. Broughton, *Going Downtown: The War against Hanoi and Washington*, (New York: Pocket Books, 1988), p79.

67 DiNardo and Hughes, *Op Cit*.

68 For further information on Computer Emergency Response Teams, see http://afcert.kelly.af.mil/ and John D. Howard, 'An Analysis of Security Incidents on the Internet', Carnegie Mellon University,1989–1995.

69 Matthew G. Devost, in a presentation on 'Infrastructure Defence', given at the 3 rd Annual SMI Conference, *Op Cit.*

70 Joint Warfare Publication 0-10, *UK Doctrine for Joint and Multinational Operations*, Ratification Draft Edition 1, 17 August 1999, Crown Copyright.

71 Group Captain D Love Deputy Director Security, Communication and Information Systems (RAF). Interview 7 June 1999, Ministry of Defence, Whitehall.

72 Economic Outlook, David Smith, in *The Sunday Times*, 22 August 1999.

73 Caddick, *Op Cit*, p.48.

74 Situational awareness (SA): Knowing where hostile and friendly forces are, and where they are not.

75 Strategic Defence Review, Supporting Essay Three, 'The Impact Of Technology', July 1998, http://www.mod.uk/policy/sdr/essconts.htm

76 Emmett, *Op Cit*, p. 22.

77 Rathmell, *Op Cit*.

78 *Ibid*.

ACKNOWLEDGEMENTS

I am indebted to a number of people, without which, this paper would not have been written. My thanks go to Group Captain Stu Peach for his support and guidance during a time when he had more than enough work to keep him busy. My appreciation also goes to Wing Commander Ian Morrison for listening to my developing theories and to Peter Osborn of Marketronic, for continually supplying me with leads. Finally, my thanks to my wife, Alison for her patience and to my three children who can now have their dad back.