Effects-Based Strategy: Operations in the Cognitive Domain

Peter Nicholson

This paper examines an increasingly significant aspect of warfare in the information age. Actions to produce near simultaneous effects in all domains of warfare have the potential to completely disrupt an adversary's ability to resist. The key change is a greatly improved capacity to operate and produce effects in the mind of the adversary and to induce changes in his behaviour – to operate in the cognitive domain. A framework for analysis based on the concept of intellectual capital is described together with comparisons between the influence this might have on the conventional forces of Western nations and emerging non-conventional threats.

The Domains of Warfare

Modern categorisations of warfare identify three separate and distinct domains of activity or actions. The physical or kinetic domain is the most familiar while more recently the emergence of an electronic domain is evident. The latter is sometimes called the information domain but this terminology is not preferred for reasons that become evident later in the discussion. But it is a third domain called the cognitive or knowledge domain that attracts more attention in recent times. It is important to recognise that these are domains of action but the effects resulting from such action are possibly manifested in another domain. In fact, the basis of an effects based strategy is to change the behaviour of the adversary – a clearly cognitive outcome. In summary, desired outcomes are satisfied using a strategy based on effects that are themselves accomplished via actions.

The physical domain is characterised by force-on-force encounters with the objective of destroying the adversary's ability to resist usually by the destruction of the enemy's military force. Generally, actions in the physical domain involve effects achieved by the concentration of force through mass. So force is the defining principle of warfare in the physical domain. Conflict between social groups has been resolved in the physical domain for most of human history. The establishment of the nation state as the dominant form of political organisation after the Treaty of Westphalia in 1648 led increasingly to the formation of national armies organised to concentrate force in the hands of the state and on the battlefield. With the invention of

gunpowder the physical effects became mainly kinetic resulting from blast, shock and fragmentation.

The meagre command and control, communications, computing, intelligence, surveillance and reconnaissance (C4ISR) capabilities available explain the singular, linear nature of warfare in the physical domain until the late industrial age (roughly the mid 20th century). The understanding of the commander of what was happening (his ISR system) was by direct observation of events that were recorded using pen and paper. The need for a fast, responsive surveillance and reconnaissance capability was of course recognised and means devised to adapt the technology of the time.

In the late 18th century the Royal Navy commissioned a class of ships called frigates that were lightly armed and much faster than the warships of the day. Before entering the Mediterranean in 1803, Nelson sent a frigate to determine whether the French fleet was in the West Indies. On its return with no sighting, Nelson deduced that the French must be in the Mediterranean and finally cornered them at Aboukir in the Battle of the Nile. Similarly, the preferred location of battlefields was not only for the field of fire or easy advance of troops but also for an observation point for the commander.

Communications were equally slow and unreliable on land. The commander exercised command and control by written or verbal instructions carried by an aide de camp on horseback to subordinate commanders. The invention of the telegraph in 1865 introduced the electronic domain of warfare and it was well in place by the First World War when wireless communications were routine. Commands were passed as Morse code, text or voice, and information received back from operational units in the same way. The communications element of the electronic domain rapidly increased in speed and capacity but until the last decade of the 20th century it was characterised by essentially point-to-point connections. This meant that the communications infrastructure reinforced the typically hierarchical command and control system of armed forces (and other forms of social organisation, including business).

Surveillance and reconnaissance capabilities improved dramatically through the middle period of the 20th century beginning with the introduction of high frequency surface wave radar by Great Britain in the Chain Home air defence radar system. The interpretation of the return signal required considerable skill on the part of the operators and the target position was plotted manually on a large table. This was the beginning of what was later known as the ‘air picture’. Microwave radar with higher resolution was routinely employed by the end of the Second World War including to some extent in aircraft. Terrestrial wide area surveillance systems were in place shortly thereafter with the deployment of long range bombers and ballistic missiles in the Cold War. Imagery was available from space by the 1960s

and in the last decades of the 20th century global coverage over wide portions of the electromagnetic spectrum became commercially available.

Exploitation of an adversary's understanding became pervasive in the electronic domain of warfare by the Second World War. Attempts to intercept signals by 'tapping' the line were apparent from the earliest days of the telegraph. With the widespread introduction of wireless to communicate with mobile forces, signal interception became a crucial part of intelligence gathering. Recognition of the possibility of interception of radio signals led to increasingly elaborate encryption and a cat-and-mouse game to break the codes. Famous examples include the British breaking the German coding by obtaining an Enigma machine and the United States Navy cracking the Japanese naval codes.

The invention of the internet fundamentally changed the electronic domain from about the last decade of the 20th century. The revolution in information and communications technology (ICT) was the main driver of this change. It is important to include both the computing and communications aspects of this revolution in any discussion of consequent outcomes. This is because the ability of computer processors to communicate directly with one another without human intervention has led directly to the importance of time in these interactions. It has also led to the need to distinguish between data and information that can be handled electronically and knowledge that requires human interaction. This point marks the beginning of a new cognitive domain of warfare. There has always been a cognitive or knowledge element of warfare but technological advances and the take-up of this technology leading to globalisation and a high degree of interconnectedness now expand this to a pervasive domain.

Command and control is in a transitional phase in the highly networked environment of the cognitive domain. This is because traditional command and control arrangements facilitate the transaction of power whereas a network facilitates lateral and diagonal information transactions that are very subversive to a hierarchical structure. The conundrum created by this situation is perhaps the greatest challenge in modern warfare.

The ICT revolution and the inexorable increase in computing capacity according to Moore's law, in conjunction with miniaturisation of the devices has significantly enhanced intelligence, surveillance and reconnaissance. Distributed processing in a wide array of smaller and smaller sensors networked to exchange and fuse data result in unprecedented situational awareness available to any node on the network. Technically speaking, all participants now potentially have access to all the information available. The converse to this new coin is the vulnerability of the network and the nodes on it to primarily electronic but also physical attack.

The main difference between this new revolution in military affairs and previous examples is that the ICT engine is a product of the commercial world rather than driven as before by military operational requirements. Hence, it is largely uncontrolled, growing and developing in an inchoate manner according to market forces rather than the direction of a central authority. Another important consequence is that the technology and the resultant capabilities are freely available to anyone or any organisation. Whereas the nation state tightly controlled warfare in the kinetic domain and to a lesser extent but still significantly in the electronic domain, now individuals, renegade groups and non-state actors can operate freely in the cognitive domain. The technology is pervasive, accessible and easily used by friends and enemies alike. In particular, the internet provides a means of communication that is almost uninterruptible and with broadband capable of carrying voice and imagery as well as text messages. Similarly, mobile telephony also carries imagery and text as well as voice with similar although not quite as extensive global coverage as the internet.

The sheer extent of the global communication network and the dependence of modern economies on it lead to vulnerability to both attack and exploitation. Computer network operations are routine for all organisations in modern economies from banks to government agencies. Defence is the first institutional reaction to counter the wide array of attacks on the network. These range from denial-of-service attacks that overwhelm the capacity of the network to malicious interference and deliberate attempts to infiltrate the system to steal, corrupt or destroy data. The ability to successfully defend one's network invariably implies the offensive capability to mount attacks against other systems. If the source of attacks against the network can be identified, a counter attack can be mounted. Increasingly, countries with advanced economies are reaching agreement to cooperate in defeating cyber-attacks using the laws of the host country but these sites can be attacked remotely if necessary.

Initially cyber-attack was readily evident: a denial-of-service attack would overwhelm the network and there was no doubt that an attack was in progress. Usually, the source of the attack could also be identified and action taken either to defend or to counter-attack. More recently, a widespread ability is evident to infiltrate a network and steal or manipulate data without easy detection. Stealing data provides information about the understanding of an adversary about the environment or the deployment of his capability and so forth. But undetected manipulation of his data provides the opportunity to distort his understanding and introduce an incorrect appreciation of the battlespace. This action in the electronic domain then has a profound effect in the cognitive leading to confusion, misunderstanding and sowing the seeds of distrust about his ISR system and his relationships.

The ICT revolution has enhanced the reach and influence of the media enormously in the early 21st century. Global communications allow direct transmission of television in near real time from any scene deemed newsworthy. This means that information about events (but not necessarily knowledge) is available to world audiences almost immediately. Through the staging of spectacular events, special interest groups and other non-state actors now have the ability to put their messages in front of target audiences and significantly influence global opinion. The Western democracies are particularly vulnerable to the manipulation and influence of electoral opinion by distorted messages that reach them unedited and without analysis as events unfold. In these circumstances, democratic governments are immediately placed in a reactive situation to correct impressions and misrepresentations that might not be a problem for authoritarian regimes.

The Hierarchy of Understanding

Our understanding of the world around us develops through four levels of awareness. The level with the lowest content is data. Data is simply the observation and recording of events in the real world. The next level is information - collection or aggregation of data that is associated in some way. The skin paint or radar primary return of an aircraft is a piece of data. Successive returns are information because each data point relates to those that precede and follow it, i.e. they are associated. Clearly, the amount of content in information increases over that of data because we can now begin to draw conclusions. In this example, the information content could include the track and speed of the aircraft and this could enable us to deduce its destination and perhaps even its departure point. The speed could lead to a deduction about the type of aircraft and hence its likely mission.

Knowledge is the next level of understanding, distinguished by the need for human interaction to interpret, explain and comprehend data and information. The main reason for this is the ability of humans to associate data and information that have no apparent relation to one another. In other more technical terms, there is no algorithm for the association and it cannot be modelled with the same degree of precision we have come to expect from our understanding of the physical world. This ability is called intuition and develops from the world view, experience and cultural influences of the person involved or in other words the social context. While there have been many advances in modelling the influence of human decision making to develop autonomous systems such as neural networks, fuzzy logic, intelligent agents and robotics, to name only a few, none have yet shown the capacity to make the leap of logic that every human accomplishes effortlessly.

The important distinction between data and information on the one hand, and knowledge on the other is that data and information can now be exchanged, categorised and manipulated electronically without the need for human intervention. This is not to say that human interpretation or clarification of data and information will never be necessary but rather that human involvement is essential to transform data and information into knowledge. There is no indication at present that technology is available or even close to fruition that can replicate the ability of the human brain to carry out this transformation.

Intellectual Capital

The concept of intellectual capital is a useful framework for analysis of the cognitive domain but is by no means the only means of examination. Intellectual capital comprises four components: structural, relationship and human capital, and intellectual property. Each of these has parallels in the business world and in social organisations more generally. Actions to defend one's intellectual capital, to attack that of the competitor, or to exploit that of a competitor or neutral party are not confined to the military arena but extend across human endeavour generally.

The structural component of intellectual capital is the explicit knowledge captured in the processes and procedures of the organisation. This includes actions to record, store, disseminate and subsequently access corporate information and knowledge. Until the widespread application of distributed computing systems in the 1980s, the structural component of intellectual capital was mostly contained in paper hard copy or in centralised mainframe computer files and usually rigorous archiving processes were in place. With the explosion of the amount of structural capital in the era of desk top computing, this rigour is often now missing resulting in poor corporate data and information archiving. Organisations in advanced economies with a high level of take-up of information and communications technology, particularly desk top computing, are probably deficient in structural capital compared with the past. On the other hand, increased complexity and the ICT revolution have allowed creation of greater amounts, so while it is probably less well organised, the quantity is greater than before. Considerable time is necessary to develop structural capital because organisational practice and procedure evolves gradually. Structural capital is thus something that develops in the same time frame as force structure and is generally not a preparedness issue.

The relationship component of intellectual capital is knowledge about the adversary or competitor, own forces, third parties and the environment, including the electronic environment. The counterpart in the commercial world is knowledge about business competitors, customers, suppliers and

sub-contractors, and the market place generally. Traditionally considered as the most valuable portion of intellectual capital because it is akin to intelligence about the enemy, relationship capital is generally perishable in a tactical sense. However, observations about patterns of activity over a longer term can lead to conclusions about behaviour and interpretation of motive and intent and form a strategic repository. In some respects, relationship capital is more a short term preparedness rather than a long term force structure matter but the time and effort necessary to develop linguistic skills and cultural awareness of existing and emerging non-conventional threats present a special case.

The human component of intellectual capital is the skills, expertise, education and training, and experience of the people involved in the dispute. Generally this is not the population at large but the leadership group and armed forces or other key groups in the society. Western societies have very strong human capital in conventional terms as evidenced by the rapid advance of technology, increase in wealth, military predominance and so forth.

The intellectual property component of intellectual capital is the beliefs, value system, shared ideas and understanding, heritage and tradition, idea of nation, and world view of a society. These elements are deeply embedded in the society and will be virtually invulnerable to attack. In fact, attack on them will likely result in an extreme reaction by the populace to defend this component of intellectual capital and support the present leadership group. So the vulnerability of the intellectual property component lies in its exploitation but this will be a very subtle and nuanced effect.

Knowledge Warfare

Knowledge warfare is about operations in the cognitive domain. It may employ kinetic and electronic effects in addition to cognitive effects but the desired outcome is to influence behaviour. Knowledge warfare involves attacking the adversary's intellectual capital, defending one's own intellectual capital against attack and exploitation, and exploiting the intellectual capital of the adversary and neutral third parties. Exploitation means learning about the content of the intellectual capital of another party without their knowledge that this is taking place. By understanding the content and extent of an adversary's intellectual capital we can identify weaknesses and strengths and better orient our capabilities in the battlespace. Exploitation can also mean altering or amending the intellectual capital of another party without them being aware that this has occurred. Through this means we can distort the adversary's understanding of the battlespace including the disposition of our capabilities and of his own forces.

There are a host of potential knowledge operations each aimed at a specific target and tailored to meet different objectives. Psychological operations target the adversary's combat forces with the objective of inducing fear and reluctance or refusal to fight. Psychological operations have a deterrent effect and can be effective against poorly trained or poorly led conventional forces. However, they are unlikely to work against highly motivated, well trained forces or against unconventional forces such as terrorists. Psychological operations take new forms in the age of the internet. Email and voice mail messages were used to good effect during the second Gulf War to warn senior Iraqi officers that they would be liable for subsequent prosecution as war criminals if they employed weapons of mass destruction.

Public affairs target the adversary population and third party opinion, increasingly world opinion, with the objective of diminishing support for the adversary regime. The intention is to convince neutral audiences of the 'badness' of the adversary regime (not its people) – the threat it poses to the international order or to particular ethnic, tribal or religious groups – and the 'goodness' of our cause. The electronic media play a large role in public affairs and recent experience indicates that truthfulness and accuracy are the most important factors. World opinion generally and Western audiences in particular are very sensitive to 'spin' and this can be counter-productive. It may be necessary to correct inaccurate or deliberately misleading reports from hostile news agencies. This can be very difficult if the incorrect reports play to preconceived ideas or prejudice. In the extreme, it may be necessary to electronically interfere with television transmissions or websites that carry an incorrect version of events.

Public relations are aimed at domestic opinion to bolster support for the political leadership and the course of action it proposes. In the Western democracies, public relations requires close interaction with elite opinion makers and elected politicians because these parliaments are likely to conduct open hearings into government actions. Anything but honesty and complete transparency will almost certainly result in loss of support and partisan manoeuvring to gain political advantage. On the other hand, public relations are less important in closed societies particularly where there is strict media control by the regime. The burgeoning of global electronic media sources makes it increasingly difficult for authoritarian regimes to control the flow of information to its people. Creating the conditions for easy access to the global electronic media may eventually be a powerful weapon for the West in influencing opinion in societies that implicitly support Islamic jihadist movements.

Camouflage, deception and subterfuge are the means to create a false understanding on the part of an adversary of the physical, electronic or cognitive environments. If successful, the loss of situational awareness caused by this can expose weaknesses and vulnerabilities that can be

exploited by concentration against weak points, economy of effort or more robust defence of own deficiencies. But a potentially more powerful effect is the cognitive disorientation and dislocation in the adversary leadership when it realises its assessments are incorrect. This can lead to mistrust of its surveillance system and intelligence processes and has the potential to reverberate through the personal networks of an organisation that relies on people rather than electronic means. This is why the infiltration of a terrorist group with the objective of providing false information is probably the best way to disrupt its operations and defeat it.

The equivalent tool where a group has greater reliance on electronic means to gather, store and disseminate surveillance data and intelligence is information operations. Information operations are defined in many ways but in essence mean the protection of own information and information infrastructure while denying the adversary unfettered use of his sources and information. Information operations also include the surreptitious manipulation of an adversary's data bases to provide false or misleading information to his intelligence system.

Cognitive Effects

Creating effects in the cognitive domain has always been part of warfare. These effects were against some or all the targets discussed above: the opposing force, the populace of the opposing nation, allies of the enemy and neutrals who might oppose or assist the adversary. The action to accomplish cognitive effects was invariably physical: offering either actual brutality and lack of mercy or the rumour of these to induce fear of retribution if opposed. Genghis Khan successfully conquered and held huge swathes of territory because of the acquiescence of the local people who feared the consequences of resisting his Mongol hordes. Centuries later very large numbers of people fled before the Soviet armies invading Germany on the rumour of the barbarities that would be inflicted on them if they stayed. In these situations, there was physical action or the threat of it against the human component of the intellectual capital with the other components remaining largely intact.

Modern societies are much more vulnerable to operations in the cognitive domain because of their higher degree of interconnectedness and the ability of adversaries to act in the electronic domain to create cognitive effects. The high level of dependence of modern societies on the electronic domain creates the conditions for substantive knowledge operations. Each of the components of intellectual capital of the society or its institutions is vulnerable in one way or another to attack and exploitation and each may be difficult to defend. The proliferation of threats from non-state actors and their inclination to apply asymmetric tactics and techniques against modern

societies creates different scenarios but no less diminishes the vulnerability of these groups to knowledge warfare. Indeed, the success of al Qa'ida and other Islamic jihadist terrorist groups is testament to their ability to operate in the cognitive domain because they are comprehensively inferior in the physical and electronic domains. The key to success against them is probably our ability to turn these same operations against these groups. It is certainly incorrect to assume that effects in the kinetic or electronic domains will lead to success.

Modern societies and their armed forces generally maintain and store their structural capital electronically and so it is vulnerable to information attack or exploitation. Very advanced forces like those of the United States are critically dependent on their structural capital to sustain deployed operations. For example logistic support, maintenance procedures, repairable item tracking, ammunition resupply and a host of other processes critical to war fighting are hosted electronically. Disruption of these systems will severely degrade the ability of these forces to operate. On the other hand, non-conventional forces such as terrorist networks, have little or no structural capital relying instead on ad hoc procedures that change more-or-less randomly and have little discernable signature. Achieving any significant effect on the intellectual capital against of a terrorist group is highly unlikely to be accomplished by targeting its structural capital.

However, one aspect of structural capital that is important to a terrorist group is its funding sources and financial management system. Improvements in surveillance of the global banking system to counter money laundering also allow detection and interception of movement of funds between the leadership group and the field operatives. This has the potential to cripple non-conventional threats by restricting their operations in space and time. The capability of any terrorist group is severely diminished without global reach and ability to strike at a time and place of their choosing.

The form of relationship capital differs markedly between Middle Eastern and Western societies and is reflected in the non-conventional threats of the Islamic jihadists and the conventional forces of the latter. The tribal, ethnic, religious and cultural background of the jihadists rely more on trusted networks of kin and less on technical means to gather, collate and pass information. This means that understanding the threat posed by these groups, i.e. the capability, motive and intent, requires deep knowledge of these 'soft' issues including linguistics, cultural awareness and family links. These soft issues have a very low signature and in the main are detectable only through human contact rather than technical means. The best tool for creating an adverse internal cognitive effect might be to sow mistrust in the personal networks.

On the other hand, Western societies and their conventional armed forces are far more transparent with readily detectable signatures. Certainly their technical capability, particularly with regard to persistent, global surveillance in the electronic domain, is unmatched. And their knowledge of own forces tends to be reasonably complete. This makes them a formidable challenge to another conventional force but of little consequence to unconventional threats that fall below their detection threshold.

The conventional forces of Western societies are generally highly skilled albeit often specialised and serve as volunteers. Despite being volunteers, the servicemen and women of Western armed forces are generally not highly motivated and increasingly see their time in uniform as a first career. Their values and belief system are sensitive to domestic electoral opinion but probably not vulnerable to propaganda or other forms of psychological operations on the part of an adversary.

Terrorist groups contain two completely different forms of human capital. One is the leadership group that is generally experienced, highly skilled and motivated having studied and practiced their field craft in several conflicts. The leadership group typically is well educated and has a deep understanding and abiding hatred of Western society. Eliminating or neutralising the human capital represented by the leadership group would likely produce a significant effect on the capability of a terrorist organisation. The second form of human capital is the field operatives presently primarily suicide bombers who are highly motivated but with generally a much more restricted world view than that of the leadership group. Intercepting this group is important in preventing a bombing but neither this nor their self destruction will make any substantial impact on the human capital component of the intellectual capital of the terrorist group as a whole.

The intellectual property of all societies includes their belief systems and values. These are embedded in the roots of their civilisation and will not be easily altered; indeed the present conflict between the West and Islamic jihadists is described as a clash of civilisations. Nevertheless, some potential leverage points are available to the West in this struggle. There seems little doubt that some aspects of Western society are very attractive to young people of the largely authoritarian societies of the mainly Middle Eastern Muslim world that harbour and support terrorist groups. These are the aspects that should be emphasised in Western public affairs targeted at young people while not questioning those that represent fundamental tenets. The full emancipation of women and democratic systems of government are two that would likely resonate with Generation Y. These cognitive effects can be delivered by electronic means and should be supported by physical effects that support the message. In particular, the disparity in wealth can be assuaged by carefully targeted aid aimed at creating economic independence and well-being rather than supporting a welfare culture.

Implementing an Effects-Based Strategy

The preceding discussion reveals some interesting aspects about operations in the cognitive domain. First, enormously increased capability in the electronic domain and the increasing reliance on this advanced technology by both modern and medieval societies greatly enhances our ability to create cognitive effects. The pervasiveness of the ICT revolution means that even the Arab street relies on television and radio for near real time news about events. Shaping and influencing public opinion is now an integral part of all conflict.

Second, actions in one domain will likely have an effect in the same and other domains. Some of these effects will be unintended or unexpected, so a much more holistic planning process must be in place for the successful implementation of any strategy. Kinetic and electronic effects can be constrained and more-or-less bounded in the targeting process but cognitive effects will touch participants, bystanders and remote observers alike. So the planning process for operations that will have cognitive effects and the actions to implement them must extend across not just whole-of-government but whole-of-nation. This is an extremely difficult if not impossible task in pluralistic democratic societies so the political leadership must mould domestic opinion to understand the complex and complicated nature of modern conflict.

Third, the interconnectedness of the modern world means that actions in all three domains of warfare will likely be widely distributed in time and space and coordination of the subsequent effects will be difficult. The fundamental principle of modern warfare is no longer force or manoeuvre but rapidity of action. The time frame of action has collapsed to a few minutes, essentially the time required for human commanders to make decisions. Actions and their effects are not sequential and linear but simultaneous and parallel, and a high degree of synchronisation is necessary for effectiveness. Achieving a coherent outcome is difficult but if achieved can have a devastating overall outcome on the adversary.

Fourth, carefully targeting of effects in the cognitive domain is necessary to minimise unintended consequences. The centre of gravity of the Western democracies is undoubtedly domestic opinion and its effect on electoral outcomes although world opinion may also be influential in countries with governments with small majorities or divided opinion. The intellectual capital of non-Western societies is very opaque to the advanced democracies and there are numerous recent examples in Afghanistan and Iraq of misreading these societies and inadvertently assisting the insurgent and terrorist cause. This field of human intelligence needs a deep understanding of the language, culture, religion and social mores of the target populace only acquired over a long period. Western comprehension of the intellectual

property of Islamic societies is a major deficiency that must be rectified to counter the jihadist terrorist groups.

Conclusion

The use of force in the kinetic domain of warfare remains important for employment against both the armed forces of nation states and emerging unconventional threats like those stemming from Islamic jihadists. These kinetic actions are much more accurately targeted and precisely delivered than ever before as a direct result of the revolution in information and communication technology. However, their effects are increasingly directed at the cognitive domain with a view to changing the behaviour of the adversary. Similarly, actions in the electronic domain are intended to produce effects in the cognitive to a greater extent than previously.

Reliance on advanced information and communications technology by both modern and more traditional societies is partly responsible for creating the conditions for more controlled actions in the cognitive domain. But examination of the elements of intellectual capital shows that not all are susceptible to effects generated in the electronic or kinetic domains. So we must devise other actions to produce effects on the intellectual capital of the adversary. This requires a much greater investment than hitherto in understanding the intellectual property aspects of adversary groups that threaten the Western democracies. These aspects include language, cultural standards, religious beliefs, ethnic backgrounds, tribal affiliations and kinship links to name just a few. Gaining knowledge of these 'soft' matters will take time, patience and sustained effort.

The importance of this is that effects in the cognitive domain have the potential to rapidly disrupt adversary operations through disruption and dislocation of his decision making and direction processes. Hence, the utility of unexpected attacks and adverse influence on the adversary's intellectual capital is a breakdown in his ability to respond. Cumulative effects achieved by coordinated actions in all three domains of warfare are widely dispersed and may appear not to be associated. This parallel, synchronised and highly non-linear style of warfare works directly on the adversary's comprehension of events in the battlespace. The paradigm of an effects based strategy directed at the cognitive domain is the speed of events overwhelming the capacity to respond. Although use of force may be threatened, action may not need to extend into the physical domain if the adversary is convinced that he is unable to pursue his chosen course of action.

New and different planning and command and control arrangements are necessary for the conventional forces of Western societies to respond effectively to the threat of extant and emerging non-conventional forces

exemplified by the Islamic jihadists. A coherent response will require a whole-of-nation approach at the grand strategic level to ensure coordination of desired effects. The adversary is a product of and generally embedded in his society. He can be identified and isolated by a determined and sustained attack on his intellectual capital. An audit of the intellectual capital of likely non-conventional adversaries to identify strengths, weaknesses and vulnerabilities would be a useful place to start.

Peter Nicholson is a founding Director of the Kokoda Foundation. He served for 33 years in the RAAF with command and staff appointments at every rank retiring as Air Vice-Marshal in 2001. He formed and led the Knowledge Staff in the Department of Defence, the first attempt in the western world to develop a coherent approach to the development of C4ISREW capability. He was made a Member of the Order of Australia in 1996 for his work as the first Joint Force Commander of Northern Command and promoted to Officer of the Order in 1999 for his work as Air Commander Australia. pgnicholson@bigpond.com.