Network Enabled Capability, Air Power and Irregular Warfare: The Israeli Air Force Experience in the Lebanon and Gaza, 2006-2009

By Group Captain Alistair Byford

Networked Enabled Capability (NEC) has been heralded as a potentially transformational capability for the effective delivery of air power, but the benefits have not always been clearly articulated. This paper uses an analysis of the Israeli Air Force's employment of networked capability in irregular warfare to argue that it can be used to either facilitate time critical targeting, or alternatively, to underpin mission sensitive targeting, where the speed of prosecution is less important than the effects that may be generated. The Israeli experience in the Lebanon and Gaza indicates the enduring importance of context, although it is possible to draw generic lessons; most notably, the Israeli Air Force's recent operations clearly demonstrate that while NEC is essential to share the information necessary to conduct an effective air campaign in the cluttered complexity of irregular warfare, technical and tactical excellence by itself cannot deliver campaign success unless linked to coherent strategy.

Introduction

The concept of Network Enabled Capability (NEC), or Network-Centric Warfare (NCW) as it is termed in the United States and Israel, has been heralded as a potentially transformational capability for the effective delivery of air power, but in the United Kingdom at least, the translation of the rhetoric into practical reality has proved to be slower and more problematic than was originally envisaged: the Ministry of Defence has even felt compelled to argue defensively in its own official handbook that 'NEC is not a pipe-dream'.[1] This paper aims to examine the potential benefits of NEC in the prosecution of irregular warfare, based on an analysis of the experience of the Hel HaAvir, the Israeli Air Force (IAF), in the conflicts with *Hezbollah* in the Lebanon in 2006 and *Hamas* in Gaza in 2009. It will be argued that at the tactical level, the shared situational awareness conferred by NEC may broadly be used to either facilitate time sensitive targeting, or alternatively, to underpin mission sensitive targeting, where the speed of prosecution is less important than the outcome and the effects - both intended and unintended – that may be generated.[2] However, the IAF's experience demonstrates that while effective NCW is an absolute necessity in the 'cluttered, complex and congested' environment typical of today's 'Fourth Generation Wars'[3], by itself it cannot be a sufficient condition for mission success; unless driven by a sound strategy and coherent campaign plan, operational excellence, however well facilitated by even the most comprehensive NEC architecture, will still result in campaign failure.

The context for the development of the IAF's NCW Capability

NCW is not new: in 1940, Fighter Command famously benefited from an integrated air defence system based on a network concept dating back to 1917. This was developed into a genuine, networked capability as technologies such as Radio Direction Finding (radar) and radio-telephony (R/T) became available in the interwar period, enabling data to be collected, filtered, fused, analysed and disseminated via a network of land-lines and ground-to-air radios. This early example of NCW provided shared situational awareness and resulted in battle-winning decision superiority.[4] What has changed subsequently is the extent and complexity of the NEC requirement, especially in expeditionary warfare, which is inevitably joint and combined - and where the international element may well be based on bespoke coalitions, rather than on long-standing Alliance partnerships benefiting from established equipment and protocols. Therefore, the United Kingdom's must develop an approach to NEC that seeks to integrate national and multinational force elements across all environments, using disparate operating systems, information resources, communications media and software tools, raising issues of ownership, protocols and security.

In contrast, the context for the IAF is significantly different and, in many ways, far simpler. Israel is a small state lacking strategic depth and the Hel HaAvir's disposition is compact and geographically concentrated; expeditionary warfare is not anticipated and operations are

invariably conducted by the Israeli Defence Forces (IDF) acting alone, from its well-established bases and infrastructure. For the IAF, this means that centralised command and control – and more than an element of centralised execution - is both possible and effective; for example, all of Israel's territorial borders are within line-of-sight airborne radio contact of the central air command post at normal operating altitudes. Consequently, the IAF has developed a tradition of centralising command at the highest level, particularly as it has a history of conflicts where tactical dilemmas have strategic impact. In the so-called 'War of Attrition', conducted between the 1967 'Six-Day' and 1973 'Yom Kippur' wars, Egyptian aircraft were often flown by Soviet pilots and tactical engagement decisions therefore created significant political consequences. Accordingly, the IAF chief of staff routinely manned the air command post personally, taking control of tactical operations and establishing a precedent for active tactical decision-making at the highest military level that continues today.[5] Additionally, Israel's well developed aerospace and electronic industries have developed many of the technical systems used by the IAF indigenously and, with little requirement to network with allies or coalition partners, the threshold of difficulty for establishing a genuine NEC is much lower than is the case for the United Kingdom.

However, despite the enduring emphasis on centralised control and the relative ease with which a comprehensive NEC could be implemented, the IAF's approach to NCW initially followed a bottom-up, tactics-led approach. This had its genesis in an early, Israeli-developed equivalent of the Link 16 network, designed to share situational awareness between fighters in air-to-air combat at the tactical level. The stimulus was provided by the small size of Israeli forces in relation to the numerical strength of actual and potential foes, driving an acute sensitivity to avoidable 'friendly-fire' incidents and a concomitant requirement for the best possible access to shared information to mitigate risk. This aversion to casualties was also one of the drivers behind the IAF's early investment in Uninhabited Air Systems (UAS) for 'dull, dirty and dangerous' tasks. This provided an additional impetus to develop networked systems, as the drone operators found that the limited field of view available from on-board cameras provided insufficient situational awareness to enable effective operation, especially in urban environments, without further information provided by off-board sensors; a sensor-to-shooter link was, in any case, necessary, to engage targets, as these early UASs could not be armed. The final tactical imperative to develop an effective NCW capability was provided by the need to develop the best possible intelligence, derived from all sources, to enable air operations within the very dense surface-to-air missile belts that were likely to be encountered in certain operating areas. For example, the IAF had to counter nineteen missile batteries in its operation to suppress the Syrian defences in the Bekaa Valley in June 1982, destroying seventeen immediately, and the remaining two the next day.[6]

Consequently, while there was never an overarching IAF NCW

programme, a number of compelling tactical imperatives combined to drive a bottom-up requirement that had produced a functioning NEC by the time of the Lebanon campaign in 2006.[7] The IAF's objective was to develop this into a capability that was useful across the three-step spectrum of conflict facing the IAF: low intensity operations, such as counter-insurgency tasks in Gaza; high intensity operations, such as air strikes against neighbouring states well-equipped with conventional forces, exemplified by *Operation Orchard*, the raid on an alleged Syrian nuclear facility in September 2008; and the most taxing mission, 'no joint border' operations against states elsewhere in the region, geographically separated from Israel by third party nations. Examples would include *Operation Babylon*, the air-strike against the Osirak nuclear reactor in Iraq in June 1981, or the mission reported in the open press that was conducted in January 2009 against an arms convoy in Sudan that was allegedly smuggling *Fajr-3* rockets into Gaza.[8] The Hel HaAvir aimed to employ its developing NCW capability primarily to underpin its centralised command and control philosophy while enhancing both its air-to-air capabilities, to counter potential opponents armed with fourth generation Western and Russian fighters in the *Flanker* or *Eagle* class, and its air-to-ground capabilities, with a particular emphasis on urban operations and the ability to engage time-critical targets, particularly rockets, pop-up surface-to-air missile threats and larger, ballistic missiles in the *Scud* class. In the event, it was the requirement to prosecute time sensitive targets that really shaped the IAF's employment of NCW in the Lebanon in 2006.

The Lebanon, 2006

The Israeli incursion into Southern Lebanon faced a new challenge in the guise of *Hezbollah*, pioneering what has subsequently termed 'hybrid warfare'.[9] *Hezbollah* is neither entirely a military force nor a terror group, instead mixing conventional, high-technology capabilities – Iranian *C-701* anti-ship missiles, suicide unmanned air vehicles, command and control nodes, remote sensors and intelligence posts – with asymmetric and terrorist strategies. The most critical requirement for the IAF was to destroy *Hezbolloh's* arsenal of some 13,000 rockets before it could be effectively deployed against Israel's civilian population in retaliation to IIDF military action. The missiles ranged from short-range *Katyusha* and *Shahins*, through the *Fajr 3-5* series, with a seventy-five kilometre range, to the long-range, *Scud*-like *Zelzal 2s*, which could strike Tel Aviv from Southern Lebanon.[10] The IAF was well aware of the time-critical nature of this task and entered the conflict with the 'one digit concept', mandating that the sensor-to-shooter cycle had to be completed within nine minutes or less.[11] Although this was considered challenging, it proved to be completely inadequate to engage the smaller, portable and mobile rockets that were fired and then moved or hidden immediately in 'shoot and scoot' tactics, often using civilian buildings, schools or mosques for cover. In practice, the requirement had to be reduced to just twenty seconds. Before the start of the conflict, this was only considered

possible if sensor and shooter were integrated within the same platform, but under the pressure of operations, the IAF demonstrated the agility and adaptability to develop its existing NEC into a system able to link multiple platforms, and routinely achieve the new target time, within just two days.[12]

There were specific circumstances that made this possible. The relatively confined geographic area of Southern Lebanon meant that a shooter, usually either a fast jet or attack helicopter, was omnipresent, on call at all times for an immediate hand-off from the sensor, usually carried onboard a unmanned air system, or based on the ground as a radar or electro-optic device. Additionally, rules of engagement were sufficiently relaxed to permit third party targeting by sensor operators of targets not positively identified by the shooter at the point of weapon release. This is a luxury that is unlikely to be available under the much more restrictive rules of engagement that exist in most Western discretionary deployments, where sensitivity to collateral damage is acute, because the maintenance of popular support - indigenous, domestic and international - is paramount. In contrast, the campaign in the Lebanon was not regarded by the Israeli public as optional, because the state had suffered 26,000 separate attacks at the hands of *Hezbollah* in the preceding six years, including 12,000 rocket firings and 1,700 improvised explosive device strikes, and the deaths of some 1,100 of its citizens. Consequently, there was a robust attitude to targeting errors and civilian casualties. It should also be noted that the twenty second sensor-to-shooter cycle was not always defined by detection to weapon release; the requirement was for the shooter to be locked on to the target within twenty seconds, which could then be tracked and prosecuted at leisure, in compliance with extant rules of engagement and often with final authorisation, at the highest-level, from the central air command post.[13]

In the Lebanon in 2006, NCW proved a tactical-technical success, underwriting the IAF's operational excellence. During the thirty-three days of the conflict, in excess of 10,000 combat sorties were flown without loss, average bombing accuracy was assessed at less than ten metres and *Hezbollah's* infrastructure was significantly degraded; it is estimated that half of its rocket stock was destroyed and upwards of 500 of its fighters killed as a result of air attack.[14] Little of this would have been possible without the networked capability that was developed adaptively at the beginning of the conflict. However, while the IAF largely neutralised the threat from long and medium-range rockets, destroying the *Zelzal 2* arsenal, for example, in a devastating and highly efficient air operation at the very beginning of the conflict, it was completely unable to prevent *Hezbollah* from continuing to use short-range rockets against the Israeli civilian populace, and an estimated 3,970 firings caused forty-three civilian deaths in Israel.[15] This eventually precipitated an unplanned, unforeseen and ill-executed land assault into Southern Lebanon, when the original strategy had been to use air power, assisted by Special Forces, to minimise the Israeli foot-print on the ground and therefore reduce casualties; the original *casus*

belli had, after all, been a retaliatory action in response to the kidnapping of two Israeli soldiers. *Hezbollah's* Director General, Hasan Nasrallah, astutely manipulated the media to maintain popular support, and the international community increasingly questioned the proportionality and discrimination of the Israeli application of lethal force, as more than 900 Lebanese civilians were estimated to have died.[16] Therefore, despite the tactical successes of the IAF in NCW-facilitated, time-critical targeting, the joint campaign faltered at the operational level, and the end result was – arguably - strategic failure. This illustrates the limits of even the most capable, technologically-based use of force, if it is applied within the bounds of a conceptually flawed plan; ultimately, ideas and strategy will always matter more than the capability or equipment. As Uzi Rubin, the founding director of Israeli Missile Defence put it:

There is no reason to disbelieve the Israeli Air Force's claim that towards the end of the war every launcher that opened fire was quickly eliminated. Yet…it may well be that all the effort that has been made to achieve this impressive technological feat was misdirected.

Operation Cast Lead - Gaza 2009

While the IAF's employment of a networked capability in the Lebanon was primarily driven by the time sensitive targeting requirement, during *Operation Cast Lead*, conducted against *Hamas* in Gaza between 27 December 2008 and 18 January 2009, the IAF sought to employ its NCW capability primarily to achieve mission sensitive targeting. Cognizant of the international outcry that had proscribed its operations in 2006, it aimed to use network capability facilitated shared situational awareness to control damage and, in particular, limit unintended effects. The extent to which it was able to achieve this would not be acceptable in current Western discretionary interventions, if legitimacy and 'campaign authority' are to be maintained,[17] but the Israelis regard the operation as a success within the terms they set themselves and believe that it could not have been conducted at all without the use of NCW.[18]

There were significant differences between the two conflicts: while the Southern Lebanon is primarily rural, Gaza is one of the most densely populated urban environments on Earth, with a population of 1.4 million confined in an area just six kilometres wide and forty kilometres long. The IAF was aware that *Hamas* would deliberately fight, in Rupert Smith's words 'amongst the people,'[19] seeking to use civilians as human shields in a bid to negate the IAF's asymmetric superiority. The IAF's objective was to demonstrate publicly that it could and would engage *Hamas* operatives despite the presence of non-combatants, and it believed that NCW provided the means to accomplish this by fusing and distributing an all-source intelligence picture to share awareness and thus minimise collateral casualties. Although actual casualty figures are hotly debated, Major-General Yoav Galant, Officer Commanding Southern Command, claimed that the Israelis killed 800 *Hamas* fighters while admitting the deaths of 200 non-combatants, proclaiming this to be an 'unprecedented ratio of success' in

this type of warfare.[20] Certainly, it was better than the results achieved in the Lebanon, but would still fall short of what would be acceptable in the majority of Western discretionary interventions.

Given the nature of the urban terrain in Gaza, operations were much lower tempo than those conducted in the Lebanon in 2006, and were predominantly intelligence-led, with most targets identified by human sources. The extent and depth of the Israeli intelligence operation is indicated by their detailed knowledge of the numbers of people using buildings in Gaza City and, sometimes, even their phone and mobile phone numbers. *Hamas* fighters often used one floor of a house, with civilians located above and below, so where possible the occupants were called by phone or texted to be warned of attack, typically being given ten minutes to vacate; sensors were used to count the numbers leaving before a strike was authorised. *Hamas* allegedly often encouraged civilians to move on to the flat roofs typical of most Gazan houses when they sensed, or were warned, that an attack was imminent. The IAF therefore developed the 'knock on the roof' tactic, where a small yield, non-fragmentary, anti-tank type weapon (typically a *Hellfire* missile with a 25lb warhead) was used at the extremity of the roof to coerce non-combatants to disperse, before 500-lb or 1000-lb class precision weapons were used to destroy the target of interest.[21] Clearly, this required the highest possible levels of networked coordination between the different agencies involved, including the ground commander and human intelligence source, usually two shooter platforms, often more than one aerial sensor platform and the air command post, which ultimately made the decision to engage. NCW was, therefore, absolutely essential in developing the shared situational awareness required to make this system work.

Unlike operations in the Lebanon, where time was the key and NCW was used to accelerate through Boyd's OODA Decision Loop[22] from 'observe' through 'orientate' and 'decide' to 'act' within twenty seconds, mission sensitivity was far more important in Gaza, so NCW was used to share and deepen awareness at each step of the cycle, rather than being used merely to increase the tempo. The requirement was not just to identify the right target and strike it at the right time in the right place, but also with the right weapon with the right fuzing; on one occasion, a *Hamas* leadership target was successfully attacked, but the *Mk 84* bomb used was disproportionally lethal, and also killed fourteen civilians in an adjacent building.[23] The complexity of NCW, which tends to be sensor-hungry, also threw the necessity for effective battlespace management into sharp relief. The Gaza strip is only six kilometres wide, and this space was filled with up to eighteen sensor platforms at any one time, in addition to the fast jet aircraft and helicopters acting as shooters. This lesson was also evident to the United Kingdom in Afghanistan, where the deployment of No.1 ACC in 2007 proved critical in providing radar coverage and air control throughout the Helmand Valley, ensuring the effective coordination and deconfliction of the many air assets that gathered whenever NATO troops came into

contact with the *Taleban*.

The IAF had learned about the pre-eminence of information in the Lebanon campaign in 2006, and took innovative steps to link proactive information operations to its kinetic activities in a bid to get on the front foot in the media war. Operational security was afforded a high level of importance: the international media was barred from the Gaza Strip and IDF personnel were not permitted to take mobile media devices into the area. However, the downside of this policy was that 'indigenous media reporters' filled the void, lacking the balanced approach that more professional news media may have brought to bear. Perhaps more interesting was the secondary campaign fought in cyberspace. Israeli civilians were recruited into active blogging teams, such as 'helpuswin.org', which set up social media war rooms to promote the Israeli cause by influencing online discussions.[24] The IDF launched its own YouTube channel to deliver a positive spin on its activities, and the site was visited more than five million times in its first week of operation. Finally, to reinforce Israeli messages and, specifically, to spread awareness of *Hamas* rocket attacks, a 'twitter' service was implemented to send 'tweets' announcing each attack.[25]

Unsurprisingly, *Hamas* information operations centred on the exploitation of collateral damage. This included the widespread staging of events for the benefit of the visual media and the use of 'fauxtography': the digital manipulation and enhancement of images. The employment of these techniques undermined *Hamas*' credibility and drew considerable criticism from the mainstream media, but despite this, and Israel's implementation of both traditional and novel approaches to information operations, it was widely accepted that Israel lost the war of perceptions at an early stage of the conflict. The key failing was centred on humanitarian issues: Israel did not permit the first delivery of aid until 5 January, nine days into the conflict, and several high visibility collateral events brought widespread condemnation from the international community.[26]

Generic Lessons

The IAF has been able to field a pragmatic and effective NCW capability quickly, by adopting an evolutionary approach rather than aiming for large-scale, transformational change. This is far from perfect, and the IAF system of integrating separately developed, discrete systems means, for example, that there is still no joint capability, with only limited connectivity available to Army helicopters. But it does mean that a workable capability has been implemented; the danger of aiming for a coherent, conceptually-driven, top-down approach is that by the time standards and protocols have been agreed, technology may have moved on again. Clearly, the implementation of NEC for the IAF is relatively simple, in that most of the systems involved have been indigenously developed and there is an existing degree of compatibility. In the United Kingdom, the issue is less clear-cut, with the necessity to network with Alliance and Coalition systems, and the concomitant problems of ownership and security protocols that this brings. However,

it would appear preferable to implement a capability early and then develop it as the concept is refined and protocols agreed; this is essentially the route that the IAF is now taking, with a tradition of platform-centred procurement being gradually superseded by a system where Command, Control, Computers and Intelligence is now being given precedence in the Equipment Capability process, building on the extant networked capability now available.

The second significant lesson from the IAF's experiences in irregular warfare is that NEC is only ever a means to an end; what is important is how it is subsequently used. Typically, this may be to either facilitate command processes or to achieve 'decision-superiority'. Essentially, at the tactical-level, networked capability can be used to either speed up the decision cycle, or to enhance it, by increasing understanding at each step. The United Kingdom's conceptual thinking still tends to emphasize the benefits of speed above all else; its vision for future operations states that 'network-enabled warfighting force elements will have the ability to operate at higher tempo.'[27] While this is patently obvious, the IAF's experience of operations in irregular and hybrid warfare indicate that in some circumstances, the speed of decision-making may be less important than the accuracy of the decisions made. This is explicitly recognized by the new fourth edition of *AP 3000*, which notes that:

There is a danger that compressing the decision cycle may in itself result in undesired consequences if observe and orientate are truncated in order to move as quickly as possible to decide and act; in this context, a focus on time-sensitive targeting (where speed is essential to prosecute fleeting targets), as opposed to mission-sensitive targeting (where the ultimate outcome is more important than the speed of prosecution) may be counterproductive.[28]

The Improved shared situational awareness facilitated by NEC is also by no means a panacea for difficult targeting decisions in irregular warfare. While NEC has huge utility in gathering and fusing the multi-source information that is required to begin to develop genuine understanding from situational awareness, the final judgment will be the choice of a decision-maker, whose perceptions will be shaped by a context involving factors including culture, strategy, legality and an understanding of the kind of war being fought and the stakes involved. Clearly, in both the Lebanon and Gaza, the IAF took risks in term of collateral damage that were acceptable in what it considered to be an unlimited war, where there was a direct threat to its own citizens, and it mitigated these risks, to some extent, by its use of NCW. However, these levels of collateral would still be unacceptable in the discretionary interventions currently conducted by the West, where popular support must be maintained.

Although the IAF's primarily tactical-led approach to Network-Centric Warfare has tended to focus this paper at the level of targeting decisions, the flow of information and awareness produced and shared by NCW may be used to enhance air command and control.

As has been indicated, the IAF's philosophy, based on its tradition and shaped by the peculiarities of its geographic circumstances, is to use this capability to enhance centralised control by providing a high-level commander with the best possible awareness to make often tactical-level decisions. However, the Western concept in irregular warfare is to take advantage of NEC to promote awareness from the top down, so that the commander's intent is more broadly understood, facilitating decentralization and a more meaningful level of genuine mission command than is currently possible.

Additionally, excessive enthusiasm about the effectiveness of NEC in irregular warfare must be tempered by the knowledge that adversaries will react – 'the enemy has a vote'. *Hamas* and *Hezbolloh* have already adapted physically, by improving their anti-unmanned air system capabilities, constraining the IAF's freedom to operate - to some extent - and degrading the intelligence picture, and also through the development of single-shot, throwaway 'fire and forget' rocket launchers, which puts the onus on detection before launch, a far more difficult problem as the infra-red bloom from rocket-firing is one of the best detection cues currently available. Deepening networked integration also potentially increases vulnerability to counter-network operations, and the IAF takes this threat seriously. The whole issue of security with regard to NEC is, however, ripe for review; the IAF takes the view that the security of networked imagery is itself time-sensitive and is only secret for the period of sense to shoot, which may be limited to as little as twenty seconds. An instructive comparison would be with the *Wehrmacht's* use of radio in the *blitzkrieg* in the West in 1940; in a very fast-moving campaign, the risk of transmitting in clear was accepted when quick and effective communication was critical. In contrast, the British and French were extremely concerned about security and insisted on a lengthy encryption process. However, by the time their messages had been decoded, the situation had often changed irredeemably and the information was irrelevant. It is clear, though, that a NEC that could be routinely compromised would be a source of huge concern. Interestingly, the failure of Russia to neutralize Georgia's air defence system as quickly as expected in the 2008 conflict may be because the Georgian system was not particularly well integrated, and therefore retained a degree of resilience to networked attack and effects-based targeting aimed at its command and control nodes.

By their very nature, air forces are peculiarly susceptible to seduction by the potential benefits of new technology. The IAF's experience, however, suggests that even the best possible technology, including NCW, will not necessarily deliver campaign success unless it is directed by an effective strategy. This is a perennial lesson of history; in the Second World War, the *Wehrmacht's* operational excellence could not deliver victory by itself, while in Vietnam, America's overwhelming technological superiority was similarly negated by its flawed strategy. The IAF was convinced that air power alone could be used to achieve the strategic objective in the Lebanon in 2006, because it believed that precision

technology, facilitated by NCW, gave it a new and transformational capability to engage time-critical targets. However, although it was ultimately able to meet the targets that it had set itself by compressing the sensor-to-shooter cycle to an unprecedented twenty seconds, this impressive tactical-technical level feat was ultimately irrelevant when Israel was perceived to have lost the war in strategic terms; as Neville Parton notes, defeat 'appears to have resulted from an over-stated belief in the impact of new technology.'[29] Similarly, while the IAF used NEC very effectively to minimize collateral damage in Gaza in 2009, demonstrating that it would not be deterred from employing its overwhelming kinetic advantage by asymmetric tactics, the short-term tactical advantage it has gained in neutering *Hamas* may well be offset strategically in the long run by the international concern that it has generated about the relatively high civilian casualty rates incurred. Therefore, the most important lesson of the IAF's experience of Network-Centric Warfare in the Lebanon and Gaza is that NEC is an absolutely necessary condition for the effective employment of air power in irregular warfare, but by itself, will never be sufficient to deliver ultimate campaign success.

Notes

[1] *JSP 777 Edition 1 'Network Enabled Capability'* (London: MoD, 2005), Foreword.
[2] *AP3000 Edition 4 'British Air and Space Doctrine'* (London: MoD, 2009), p. 17.
[3] Third Generation warfare is conventional, all-arms, force on force manoeuvre war, Four Generation Warfare is the networked, irregular asymmetric warfare of the contemporary operational environment. Thomas X Hammes, *The Sling and the Stone: On War in the 21st Century* (Osceola, WI: Zenith, 2006), p. 5.
[4] *ibid*, p. 76.
[5] Colonel Gur Laish, 'NEC and Hybrid Opponents', Lecture at Netherlands Armed Forces Conference *Future Force 2020: Are we Prepared*, The Hague, 16 March 2009.
[6] Matthew Hurley, 'The Bekaa Valley Air Battle June 1982: Lessons Mislearned?' *Air Power Journal*, Winter 1989.
[7] Gur Laish, 'NEC and Hybrid Opponents'.
[8] 'Israeli Drones Destroy Rocket-Smuggling Convoy in Sudan', *Sunday Times*, 22 March 2009.
[9] *Joint Doctrine Note 02/08 'Air-Land Integration'*, (DCDC, 2008).
[10] *Hezbolloh's Rockets* at **http://www.bbc.co.uk/1/hi/world/middle-east/5187974.stm** last accessed 1 April 2009.
[11] Gur Laish, 'NEC and Hybrid Opponents'.
[12] *Ibid*.
[13] Gur Laish, 'NEC and Hybrid Opponents'.
[14] Kainikara and Parkin, *Pathways to Victory*, p. 76.
[15] *Casualty Figures in the 2006 Israeli-Hezbollah Conflict* at **http://www.web.amnesty.org/library/index/ENGMEO20252006?open&of+ENG-cbn** last accessed 1 April 2009.
[16] Neville Parton, 'Israel's 2006 Campaign in the Lebanon', *Air Power Review*, Vol.11, No. 2, Winter 2007, p. 86.
[17] Consideration was given to adding 'Campaign Authority' as a principle of war in *British Defence Doctrine Edition 3*.

[18] Gur Laish, 'NEC and Hybrid Opponents'.
[19] Rupert Smith, *The Utility of Force* (London: Penguin, 2005).
[20] *Cast Lead Death Ratio an Achievement*, **http://www.jpost.com/servlet/satellite?pagename=JPost/JPArticle/ShowFull&cid=1237727530093** last accessed 1 April 2009.
[21] Gur Laish, 'NEC and Hybrid Opponents'.
[22] Defense and the National Interest, **http:/www.d-n-i.net/Richards/boyds_ooda_loop.ppt**, accessed 20 February 2008.
[23] Gur Laish, 'NEC and Hybrid Opponents'.
[24] Air Warfare Centre Air Warfare Group, unpublished paper, *The 2008/09 Gaza Conflict – an Analysis*, 2009.
[25] Twitter is a free social networking and micro-blogging service that enables its users to send and read other users' updates known as tweets. Tweets are text-based posts of up to 140 characters in length which are displayed on the user's profile page and delivered to other users who have subscribed to them (known as followers).
[26] *Ibid*.
[27] Gur Laish, 'NEC and Hybrid Opponents'.
[28] *AP3000 Edition 4*, p. 56
[29] Neville Parton, 'Israel's 2006 Campaign in the Lebanon', p 88.