The RUSI Journal
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rusi20

THE DIGITAL BATTLEFIELD

James E Shircliffe Jr

Available online: 22 Dec 2010

To cite this article: James E Shircliffe Jr (2010): THE DIGITAL BATTLEFIELD, The RUSI Journal, 155:6, 22-27

To link to this article: http://dx.doi.org/10.1080/03071847.2010.542665

THE RUSI JOURNAL

THE DIGITAL BATTLEFIELD

PREPARING FOR PARITY

JAMES E SHIRCLIFFE JR

The US Army has become too reliant on information systems: a major risk when it operates in environments where it cannot assure information superiority, or when it cannot support its voracious logistical requirements in the field. Infantry training must take into account that only parity, not supremacy, is possible, argues James E Shircliffe, and soldiers must be taught how to fight once again without advanced electronic aids.

It is questionable whether the US Army can still fight without 'the Network'. It is evident that today's army has become entirely addicted to the data links, both wired and wireless, that make up the Network, bringing with it dependency on electronics hardware, software and ever-growing amounts of energy. Information and Communication Technology (ICT) systems have gone from a force multiplier to being seen as a war-fighting imperative that maintains the combat capability needed by brigades for current missions. And calls come for more data processing and more powerful computers with faster connections in smaller boxes, especially as the demand to push real-time intelligence, surveillance and reconnaissance (ISR) feeds to lower echelons is forcing the army to move from handling terabytes to petabytes of data.

Much of the current training provided to army personnel, who are increasingly referred to as the 'wetware' of the Network, is on how to exploit information supremacy provided by ICT systems in an electronically uncontested environment. The army's possession of information supremacy assumes unfettered access to the electromagnetic spectrum, trusted microelectronics and software, and the ability to move as much energy – to power these electronics – into every part of a theatre as required. Yet potential future adversaries have already learnt lessons from Iraq and Afghanistan on how to asymmetrically oppose, penetrate, exploit and mimic ICT systems and their supporting logistics tail. The army has not prepared its brigades or battalions to operate without access (or with intermittent access) to the data network, nor operate with a network that has been compromised. The US Army has joined the rest of the armed services and the Department of Defense (DoD) in recognising that its information dominance is at risk. The US Army has hence started to revive its electronic warfare capability (long in hibernation), and begun to tackle cyber operations and network security, increase energy efficiency, and investigate its supply chain vulnerabilities. While these actions are necessary, the army has yet to face the uncomfortable notion that it may be called upon to operate along the full spectrum of operations without its ICT systems. In such a situation, success will depend on the fighting spirit, initiative and self-confidence of the officer and non-commissioned officer corps, all of which must be cultivated during home-based training to prepare forces for the modern battlefield in which enemies may have equal, if not supreme, cyber capabilities.

The Evolution of Network Addiction

In the 1980s, the US Army was focused on how to defend the Fulda Gap in Northern Germany from the armoured thrusts of the Soviets and the Warsaw Pact. All of the army's training resources and imagination was focused on that singular task. Other potential theatres of war, such as the Korean Peninsula and the Middle East, were expected to be smaller-scale replicas of the Fulda Gap scenario. The 1980s was also the time that the army began to conceptualise and bring to fruition its concepts of 'AirLand Battle' and the digitisation of its forces. But though it may have embraced the concepts, it did not do so wholeheartedly: when the US V Corps practised its war games in West Germany, the referees would still call for 'radio silence' – an admission that it was possible for the Soviets to deny communication. Survival would depend on V Corps's ability to operate without its data links against a foe that outnumbered them and would have the element of the surprise.

The entire conceptual construct of information dominance traces its lineage to three factors at the end of the 1970s: first, the US requirement to defeat armoured spearheads with a numerically inferior force; second, the unacceptability of first use of nuclear weapons; and third, the revolution in microelectronics manufacturing. The US has traditionally opposed the maintenance of a large standing army, regardless of the types of global commitments it has assumed, due to the primacy of affordability considerations in defence planning. Since the end of the Second World War

 DOI: 10.1080/03071847.2010.542665

In the rugged terrain of Afghanistan, a satellite communication system is set up by a US soldier during a firefight in August 2010. *Photo courtesy of Department of Defense/Russell Gilchrest*.

and the Korean War, the army has turned to technology to enhance unit firepower as a means to decrease manpower requirements. This was epitomised in President Dwight D Eisenhower's famous phrase, 'more bang for the buck', and the army's subsequent incorporation of tactical nuclear weapons into the Pentomic and ROAD divisions, formations designed to fight on a nuclear battlefield.

However, the use of nuclear weapons as a substitute for conventional firepower carried with it certain political concerns: most particularly, over the potential escalation of a Soviet incursion in West Germany into a global thermonuclear war. The Kennedy administration developed the concept of 'flexible response' as a substitute for Eisenhower's 'massive retaliation' and its connotations of a balance of terror. The idea was to be able to fight and win at every level of conflict. But, while defence spending increased to ramp up the size of the military, the Southeast Asian theatre absorbed all the extra resources, fostering doubt that the US could stand against the Soviets without turning to nuclear weapons.

The army has turned to technology to enhance unit firepower

The winding down of the Vietnam War signalled the beginning of a period of retraction by the army and a search for a mission focus to serve as the intellectual grounding around which the army could rally. The army as a cultural institution desired a return to a simpler and more inspirational concept of war based upon a shared historical perception of the Second World War, with its large tactical formations and armoured columns. This was part of a desire to break with the stigma of Vietnam that had brought such disapproving attention from the public and Congress, the holders of the purse strings. Those purse strings would have to be loosened if the army was going to modernise its weapons inventory, which had remained stagnant during the Vietnam War, as the immediate needs of that campaign drained development funds.

The question of how to actually shape the army for the 1970s and 1980s was inspired by the performance of the Israeli army in the 1973 Yom Kippur War. The work of Generals Eugene DuPuy and Donn Starry while they were in command of US Army Training and Doctrine Command (TRADOC) led the way to the development of the AirLand Battle Doctrine. This incorporated the improved lethality and precision of modern weapons in combined arms operations, and was designed to blunt the attacks of armoured spearheads and attrite second-echelon forces; crucially, it embodied tactical manoeuvrability. The end result was the ability to cause the same level of force degradation of the Soviet forces as would be achieved through the use of nuclear weapons; now, however, this would be done through the application of superior firepower at the right place at the right time. This was

made possible by the incorporation of advanced sensors and automated fire-control systems, distributed in numerous ground and air platforms. This was in turn made possible by the microelectronics revolution in Silicon Valley that decreased the size and price of computational and communication systems while also increasing their performance.

Though initiated by the US, the Soviets were actually the first to recognise the revolutionary implications of the incorporation of sensors and precision munitions on the conduct of war. It was Marshal Nikolai V Ogarkov who coined the term 'Reconnaissance-Strike Complex' to describe what the Soviets saw as a fundamental change in warfare. But it was the performance of the US in Operations *Desert Storm* and *Desert Shield* that brought the technological achievements to the attention of the DoD, Congress, the American people and the world. The major lesson was that technological quality had demonstrated that it could be a substitute for quantity – of both materiel and personnel. This shift was documented in Andrew F Krepinevich's 1992 study, 'The Military-Technical Revolution: A Preliminary Assessment',[1] as part of the DoD's effort to grasp the significance of the change. But it was Andrew Marshall who rebranded it the 'Revolution in Military Affairs', taking the focus from the technological nature of the revolution – and the Soviet origins of the term – to place it instead on the holistic interaction between new technologies, concepts for the employment of that technology, and the structure of the units that wielded it. *Desert Storm* seemed to be positive proof that technological quality could substitute for material quantity. This would be epitomised in the writings of Admiral Arthur Czebrowski, who developed the concept of 'Network-Centric Warfare' that has gained currency throughout the world's militaries.

With the collapse of the Soviet Union and the apparent invincibility of the US military, Congress sought a peace dividend in the form of cost savings derived from a reduction in the size of the standing army. This began a vicious circle whereby the army would integrate more ICT systems to increase the combat power of its brigades, which apparently justified decreasing the numbers of troops, encouraging the adoption of more ICT systems. The idea that the army would ever lose access to the electromagnetic spectrum or face a peer or near-peer competitor was never considered credible. Rather, it was assumed that the US would always maintain technological supremacy – despite its lack of expenditure in the areas of electronic warfare, cyber-security or creating trusted systems.

The Network Giveth and the Network Taketh

While much has been made about how the integration of ICT into a force can enhance operational capability, there has been little focus on the price that must be paid in resource requirements. These requirements create the potential for unexpected vulnerabilities, which could cripple a force unprepared to deal with them.

It was assumed that the US would always maintain technological supremacy

The most notable vulnerability is a matter of nature and physics: the radio frequency spectrum is finite. Soldiers, Strykers and Apaches cannot tow miles-long stretches of cable behind them in order to receive and transmit data, so it has to be done wirelessly. The radio frequency spectrum is a limited resource in demand by many users – civilian and military, friendly and unfriendly. The dependence on moving large amounts of data without a fixed infrastructure has made the DoD one of the biggest consumers of the spectrum in the world. But not all frequencies belong to the DoD in all locations.

The problem is already getting worse as the army tries to move to real-time, persistent surveillance: more wireless systems are attached to more platforms to push back more data to more users. In the past, the army could deploy a force anywhere outside of major US or Western European cities and never worry about signal collisions in communication channels. But over the last fifteen years, almost every country in the world has been rolling out wireless broadband systems as a cheap fix to the problem of connecting people without the physical infrastructure. Further, certain wavelengths are preferable to others in particular environments depending on the requirement, meaning numerous military entities are in conflict over limited amounts of bandwidth. Added to this is that the best 'bands' for the military – those that are essential for operations in complex terrain with non-line-of-sight transmission – are also desired by the commercial sector, particularly the cellular/mobile phone bands. This means that in future mission spaces, disparate organisations, whether allied, enemy or neutral, will compete for access to the spectrum.

As the US quickly learned in Iraq, and is learning again in Afghanistan, spectrum congestion follows economic development. It is difficult enough to get the DoD enterprise to co-ordinate and de-conflict spectrum usage amongst its own communications officers (let alone electronic warfare and intelligence actors), but when IraqTel employees are throwing up GSM towers in neighbourhoods seemingly at random, and at full broadcast power, an extra layer of complexity is soon added.

The best 'bands' are also desired by the commercial sector

In practical terms, spectrum managers in military bases do not have any spectrum in which to expand. In areas of poor spectrum management and enforcement – such as Iraq – 'spectrum fratricide' is a frequent problem: in other words, conflict over the electronic landscape. Spectrum managers in Iraq, for example, were surprised to discover that jammers had been introduced into the theatre in order to prevent the detonation of improvised explosive devices. The jammers, however, which they had not been told about, happened to block convoy communications.

The second serious problem in theatre is the energy profile of networked soldiers. By packing as much data into a communication link as possible, US forces emit a large amount of energy. On the battlefield, it is possible to identify any unit emitting electromagnetic energy, a tell-tale sign of communications – in Afghanistan, two brigade combat teams will have over 75,000 electromagnetic emitters of some form, making them hot targets for an enemy who can simply use off-the-shelf spectrum analysers to triangulate their position. As the saying goes, 'the chatty node gets the fire'.

Determining Trust

The US Army takes its unrestricted access to radio frequency bandwith for granted, assuming that it could find a technical fix were it to encounter problems. Rather than confidence in its systems and capability, however, this suggests a dangerous myopia about the systems trusted to collect, process and exchange unaltered data.

Any network can be compromised and exploited

A serious question continues to nag at the US security community: can these systems in fact be trusted? The drive to decrease the costs of ICT systems has led to the wholesale adoption of commercial, off-the-shelf hardware and software by the research, development and acquisition community. But the ability to consistently and continuously determine the pedigree or origin of all this software and hardware remains elusive. Every DoD science and technology conference makes reference to Tom Friedman's work, *The World is Flat*, in which he outlines the global supply chain that creates his laptop. Likewise there is niche specialisation in the production of every component of the DoD electronic network, but the question remains as to how to ensure the supply chain has not been penetrated, or harmful or malicious code or components inserted into the equipment before acquisition. The problem is complicated by the fact that commercial providers seek a profit, meaning that designs and components can change according to costs: in some cases, the printed circuit boards in a computer one week carry a different design to those from two weeks earlier.

The second issue is that off-the-shelf software is designed for communication and integration, not security. It consists of tens of thousands to millions of lines of computer code, which, as technology stands, presents an insurmountable task to validate the true functions of the software. The most common way of making commercial software secure is to strip out unwanted application functionalities, or the associated lines of code, thus reducing the places where malicious software could hide, and then securing the remaining software. Nevertheless, it is still a stripped-down patchwork of code. Given enough time, any network – wired or wireless – can be compromised and exploited. As Major General Suzanne Vautrinot, commander of the Joint Task Force Global Network Operations, once said, 'the best way to make sure a network is secure and won't hurt you is to leave it in the box'.

How can trusted systems be built from untrustworthy components? Currently, the only way to test if an integrated circuit can be trusted is to analyse it layer-by-layer as you destroy it. In other words, you know whether you had a trusted component but now it is dust. The Defense Advanced Research Projects Agency and the Intelligence Advanced Research Projects Agency are currently working on trust programmes that compare delivered chip sets with the design specifications requested to see if anything has been altered. However, this assumes a fault has not been inserted during the design stage.

The insertion of faults into software is much more difficult to test: it is currently impossible to go through every line of code and verify all of its functions, particularly if the enemy may have access to the massive resources of organised crime or a nation-state. The insertion of malicious faults, kill switches, back doors and logic bombs into software and hardware has always been talked about in hushed tones in the Pentagon, and the possibility that Israel compromised Syrian air defence radar to enable its successful 2007 air strike highlighted the strategic implications of such compromises.[2]

A Heavy Load

An unintended effect of digitisation is its impact on tactical mobility and forward sustainability. ICT systems can be bulky, heavy and power-hungry, a problem in-theatre. In remote parts of Afghanistan, for instance, some combat operations have been inhibited because the forces on the ground could not generate enough electricity to maintain their operational tempo. Army tank drivers are used to considering the risks of over-extension (sobered by the fate of Erwin Rommel's Afrika Korps, which advanced beyond the capability of its supply lines in the Second World War), but now the infantry must also do so. Soldiers must think in terms of how they march and fight on both their stomach (biological energy) and batteries (chemical energy). The addition of tactical radios, amongst other electronic accoutrements, has increased the combat load of the standard patrol as well the variety of unique batteries that must be maintained and carried. (This load will only increase as the Rifleman Radio is introduced and quadruples the battery consumption of an infantry company.)

ICT systems can be bulky, heavy and power-hungry

This was not a noticeable issue in Iraq, where soldiers could charge their batteries before a mission, or manoeuvre out of their base and return the same day to replenish their supplies. In Afghanistan, a patrol is away from its forward operating base or expeditionary camp for an average of three days, and has to carry all the batteries it needs, pushing the combat load, including armour and heavy weapons, above the weight of some soldiers. The problem is worse in the forward operating bases and air bases, as the command centres serving the soldiers require hundreds of gallons of fuel to keep their equipment powered and cooled.[3] This

has meant that the logistics train into and throughout the theatre has become larger than anticipated; it is a source of vulnerability that requires pulling troops off combat missions to mitigate.[4]

Fix Bayonets!

The US Army's *Field Manual 7-0: Training for Full Spectrum Operations* recognises that an adversary's adoption of new technologies represents a potential disruptive threat to the US advantage in key operational domains.[5] The document recognises that war is essentially a human endeavour, meaning the 'fog of war' will never be eliminated; nonetheless, it ties future success to the ability to adopt new technologies and technical innovations more quickly than the enemy.[6] This kind of thinking is risky in failing to consider the possibility of failure in the acquisition system, ICT systems or the imagination of future military officers. It is a reflection of an unspoken assumption and blind hope that the US will always have technological superiority over its opponents. More broadly, it demonstrates hubris borne from a belief in the infallibility of American ingenuity and innovation, and the sanctity of its inventions – because it has always been that way, and anything else is inconceivable. But in reality, the global proliferation of technology and scientific expertise has reached the point where the US Army, let alone the US government, cannot accurately assess whether it still maintains a technological lead.

The ICT system needs to have its own version of 'fix bayonets'

Technology currently drives the focus of training and experimentation. Every scenario experimented with and trained for assumes that the US force will always have superior ICT systems. Any problems encountered are translated into critiques of how the ICT systems, or some other technological element, can be improved; how tactics, techniques and procedures can be altered to better take advantage of the ICT systems; or a new technological priority for acquisition set. What has not occurred is the development of tactics, doctrine or training that focuses on preparing soldiers for engagements in which they will face technologically equal or superior forces, or a contested electromagnetic environment – a reasonable assumption if the army is to train for the full spectrum of operations in the face of present and future disruptive technologies and asymmetric tactics (as indeed the army claims it wants to in its own doctrine).

Soldiers need to be able to function with varying levels of ICT systems integration on the current and future battlefield, as well as without networked technology altogether. In other words, the ICT system needs to have its own version of the command 'fix bayonets'. The attachment of the bayonet to a rifle represents the backwards compatibility of that weapon system with the edged weapons that dominated the battlefield before the rise of gunpowder. While considered largely superfluous by the army today (but not the Marine Corps), the bayonet is maintained because there are situations in which a soldier will be without ammunition (perhaps due to supply chain failure or envelopment) or in close-quarter engagements. US troops have recently encountered such occurrences in Iraq and Afghanistan, despite earlier proclamations that such a thing would never occur to a US military force in modern wars.[7]

Flexible, Adaptive, Scalable

Units cycling through training evolutions today need to confront the same mission set with and without ICT systems, with and without a contested electromagnetic environment, and against an opponent equipped with inferior or superior ICT systems of their own. This requires a paradigm shift in thinking, away from a platform-centric or even network-centric focus, to a human-organisation-centric model. This will not be a popular notion in the acquisition community, whose presentations start off by talking about putting the soldier first, but quickly devolve into talking about schedule, cost, budget and getting soldiers to use the systems properly. A soldier is more than an individual; he is an extension of his unit, and a unit should be allowed to fight how the unit sees fit, not in the way that would most optimally use network resources. This will prove to be relatively easy with units at the platoon and squad level, where physical proximity allows for unit cohesion through visual and voice contact. But the problem is more difficult for modern battalions and brigades, given the size of the modern area of responsibility and the spectrum of complex tasks they must accomplish at the same time.

A soldier is more than an individual

What units need is the ability to scale their reliance on ICT systems based on specific mission requirements and threat intelligence. This is a similar concept to the idea of scalable, add-on armour being developed for armoured forces. Scalable ICT systems mean that a commander should be able to select the ICT system mix and load based on the mission criteria, the size of the area of responsibility, troop density, expected bandwidth availability, energy availability, the nature of the local threat and the leader's appetite for risk. Thus, if a commander knows the spectrum is denied to him, or that his soldiers are too weighed down to pursue elusive tribal insurgents, he could cut loose from his logistics train and form a flying column to conduct deep, dismounted infantry strikes in rugged terrain. Or, if operating in urban terrain with the support of EA-18G Growler and RC-135 Rivet Joint aircraft, a commander could load up on ICT systems.

In any scenario, the achievement of situational awareness and a shared operational picture with the minimum of communication is the epitome of operational performance, but it is rarely realised. In reality, the desire to push ICT systems into the hands of every soldier is driven by the fear that, in actual combat situations, mistakes will be made due to a failure to understand the commander's intent or establish situational awareness. Military officers with the genius of General George Patton or Lieutenant General Harold Moore are rare. Instead, the system is designed to equate

certainty of action with sufficient information, even if it could now be argued that the US Army has passed the point of simply overloading their commanders with information to drowning them in it. But instead of rebelling against this flood of information that can paralyse decision-making, many have become dependent on or addicted to their digital feeds. They thus appear paralysed without them.

Home-based training rarely encourages learning through failure, and forces are being led to believe that their ICT systems are always right – despite the frequent reminders that they are prone to internal errors and malicious manipulation. It is unlikely that a soldier will doubt what his blue-force tracker (BFT) tells him about the location of friendly forces, even if these same friendly forces tell him over a radio link that the BFT is wrong. Every training exercise should emphasise the necessity to operate quickly, and that personal responsibility and decisiveness cannot be abdicated to a machine.

Conclusion

Current army and DoD doctrine and strategic plans assume that no competitor could ever impede US information supremacy. These are assumptions that should be questioned in a world where the knowledge and components to build signals intercept platforms, GPS spoofers, digital radio frequency memory jammers and network hacking tools can be acquired on the Internet. Countries that could be the potential opponents of tomorrow are the same ones that sell the army hardware and software of unknown pedigree that cannot be inspected for trustworthiness.

Personal responsibility cannot be abdicated to a machine

The problems described above are not overwhelming, and can be addressed by proper training for troops and imaginative strategic planning in the defence administration. The time for brigades and battalions to discover how to operate when their ICT systems are denied, degraded or disrupted is at home, not in forward deployed areas. But the US Army appears to be building a force that is forgetting how to fight without its technology – despite the aphorism that a military can never afford to lose its ability to operate in a worst-case scenario. Today, that means an enemy that can dominate the networked environment, and one that can determine how future engagements will unfold: they may not fight the way you want them to or expect them to. The US Army needs to relearn the lesson that victory starts with training in the fundamentals: self-reliance, aggressiveness, decisiveness and intellectual independence – the very skills needed when kit fails and plans unravel. ■

James E Shircliffe Jr currently works as a programme manager for the Federal Bureau of Investigation. He previously worked for a variety of intelligence community agencies in Washington, DC. He holds two Bachelor's degrees from the Virginia Military Institute and earned his Master's in strategic intelligence from the American Military University. He is a member of the International Institute for Strategic Studies, the National Defense Industrial Association and the Military Operations Research Society.

The opinions and comments of the author are his own and do not reflect the position of the US government.

NOTES

1 Andrew F Krepenevich Jr, 'The Military-Technical Revolution: A Preliminary Assessment', Office of Net Assessment, Unpublished Manuscript, July 1992. A later edition (2002) is available at <http://www.csbaonline.org/4Publications/PubLibrary/R.20021002.MTR/R.20021002.MTR.pdf>.

2 Sally Adee, 'The Hunt for the Kill Switch', *Ieee.org*, <http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>, accessed 7 July 2010.

3 Although in Afghanistan, water is a much larger logistical burden than fuel, oil and batteries.

4 This is not to mention the political considerations of maintaining multiple logistical pathways through countries of questionable reliability.

5 Barry Leonard, *Training for Full Spectrum Operations: US Army Field Manual 7.0* (Fort Leavenworth, KS: DIANE Publishing, 2009), pp. 1–2.

6 *Ibid*.

7 Though in the same theatre as US forces, the Argyll and Sutherland Highlanders used a bayonet charge to sweep an insurgent position in Iraq in 2004.

ERRATUM

NATO's First Prime Minister: Rasmussen's Leadership Surge
By Ryan C Hendrickson
Vol. 155, No. 5, October/November 2010

Anders Fogh Rasmussen is the first sitting prime minister to be considered and subsequently selected as NATO secretary general, not the first prime minister to take up the post.