

Could microchips replace our men and machine guns on the next front line?

Doron Arazi

Published: 23 April 2004

A recent conference considered the idea that nations will wage war with IT rather than conventional arms but, Doron Arazi says, few were won over

The war in Iraq has highlighted the potential that high technology can bring to the battlefield, such as smart bombs targeted by soldiers on the ground using computers that can relay information to remote command centres.

But do such advances mean that information technology may eventually replace conventional warfare? Hull University's Centre for Security Studies assembled a select group of thinkers from academia, the military and business to consider the prospect.

Since its establishment in 1993, far from the London strategic studies crowd, the centre has sought to blend history and theory with practical policy advice to the powers that be. Its director, naval historian Eric Grove, regularly serves as a defence consultant for television documentaries and Ministry of Defence projects. He has practised the much-vaunted cooperation between academia, government and business by tapping sponsorships from the Royal Navy and from Hi-Q Ltd, a Wiltshire information systems company. And he press-ganged into the brainstorming exercise not only the academic educators, but also the military "doctrinators" - the senior officers from the armed services' Defence Studies Directorates, which is charged with shaping Britain's battle doctrine in the light of the lessons from Iraq. Some of them came with fresh and disturbing combat experience.

The context of the discussion was the US' massive investment in battlespace information and communication systems that complement a switch to lighter, faster, agile forces of the kind that so easily subdued Saddam's army. The UK calls it "network-enabled capability". The aim is to create "battlespace information superiority" through a "network of networks", linking all the military's decision-makers, computers, sensors, communications and weapon systems in an omnipresent, omniscient war machine that knows at all times where the enemy is and destroys him from a safe distance. But the technology was developed before anyone knew quite what to do with it, and no theoreticians could agree on the definition of network-enabled capability.

Roberto Desimone, from defence systems contractor QinetiQ, tried to disperse the confusion. It is not just about linking existing systems, he insisted. In an ever-more complex world, it is difficult to understand exactly who the enemy is and when and where threats will emerge. Aggressor states and terror networks can acquire ever cheaper

advanced technology.

Different military force "packages" must be deployed rapidly in response to unexpected crises. And coalition warfare necessitates sharing intelligence while maintaining national security.

Network-enabled informatics - based on artificial intelligence, machine learning, neural networks and genetic algorithms - would allow the integration of all available knowledge from every corner of the system into a radically improved planning process for military operations and crises.

Presenting military planning tools developed in collaboration with Edinburgh University's Artificial Intelligence Applications Institute, Desimone envisaged a holistic system that would allow all commanders to share their aims and rationale. It would highlight resource bottlenecks and resolve allocation conflicts; it would allow for dynamic revisions of plans in a changing situation; it would identify not just one or two possible plans of action but a whole array of plausible ones; it would ensure that they are consistent at all levels; and it would outline the critical intelligence needed to execute them. "Agent" systems, based on the logic of internet search engines, would allow intelligence analysts to hunt for relevant information in the whole system's vast memory instead of waiting for snippets to be fed to them through their command and communication channels. All this would depend on an "ontology" - a higher-level theory of sharing information.

Desimone stressed the current technological and human barriers to this "information superiority". And he gloomily lamented the lengthy, labyrinthine defence procurement cycle, which means that current systems are based on 1990s technology and that today's technology cannot come into military use before 2020, at best.

Kees van Haperen from Hi-Q made the point that information was not knowledge and that conventional systems thinking regarded knowledge too much as the product of a linear chain of information analysis. He believes there will always be too much or too little information, it will always be messy and partial, and its interpretation will depend on the psychology of shared culture. If information superiority is the Holy Grail, he said, the search for it must concentrate more on "what" the information is for than on how to get it.

He spoke about the Army's joint effect tactical targeting system. It had started conventionally enough, he said, as a project to coordinate battlefield fire support, but it had come up against a lack of coherence between an array of disparate information and communication systems. To effectively transfer data between them, it was not enough to merely introduce new gadgets and software; the development process had to create an overarching concept of the army's "business", break it down to "business areas" and identify the needs of "stakeholders".

Non-techie academics and soldiers are sceptical about the systems that are emerging. At the conference, the discussion centred around the example of uninhabited aerial vehicles (UAVs) - in the old acronym the "U" stood for "unmanned", but the MoD decided it was not "inclusive".

For military historian Humphry Crum Ewing, the basic parameters of getting an eye in the sky have not changed in principle from the early observation balloons to Britain's own current - and troubled - UAV procurement programmes, Astor (advanced stand-off radar) and "Watchkeeper". The problems of getting an aerial observation platform, relaying

information to base and accurately interpreting it were always the same, he said. And the practitioners from the armed services, while enthusiastic about UAVs'

achievements in Iraq, were too immersed in the struggle with the practicalities of their use to see them as a panacea.

An officer added: "Systems do not kill - men (and, increasingly, women) do." It is the fighting men and women who are most aware of the awesome moral responsibility of organised killing, and therefore least likely to be swayed by tech-talk and its implied promise of sanitising war. Ultimately, a man or woman makes the decision, so it was no surprise that officers wondered if the "knowledge-based" tag was merely "a new manufacturers' spin on data management". "You cannot frighten the enemy into submission by sophisticated analysis alone," one officer said. So by all means let the geeks supply troops with the best technology; but, even at its best, highfalutin "network-enabled capability" may be just another name for old-fashioned military common sense.

The Hull Security Conference took place on April 5-6.
