Integration: The Challenge of Knowledge Operations in 2020 and Beyond

Christopher Ankersen
Department of International Relations
London School of Economics and Political Science
Houghton Street, London
WC2A 2AE
United Kingdom

Abstract

The world of 2020 is envisaged as being either dominated by state conflict, or suffering from violence inflicted by sub-state and non-state actors. Notwithstanding which ever view turns out to be correct, several common challenges will face Western militaries. In short, the enemies of the future will be smaller, faster, less discrete and more dispersed than traditional battlefield conceptualizations allow.

In order to meet those challenges, any number of technological developments will be brought to bear. Suffice it to say, in twenty years, almost any technology will be possible—from nanotechnology to space based weapons. What will be key, however, will not be the specific gadgetry, but rather the approach that militaries take in dealing with them.

Traditionally, military technology has been developed in isolation and only 'networked' after the fact. What will be required in the future is a perspective that sees the entire system (made up of capabilities, processes, organizations, and technology) as needing to be designed holistically. In order to make this sea change in attitude and aptitude, militaries should consider employing professional systems integrators from the private sector.

Introduction

"How will we know?" The answer to this question, so evidently puzzling after the events of September 11th, will prove to be elusive even twenty years from now. By that time, despite advances in technology and changes in the geopolitical context in which armies will find themselves, *certainty* will still be an ideal, rather than an everyday condition. Commanders will continue to struggle with the thorny issues of communication, decision-making, information gathering, and defining the intent—the critical 'next move'—of the opposition. Despite our best efforts, whilst we will be able to see 'the other side of the mountain', clear, unambiguous, and relevant intelligence will not be something that the ground commander of 2020 can take for granted. The fog of war will not have lifted. Contrary to what may pass as common sense today, however, this will result in one of the strengths of military operations, an enduring theme throughout the ages, connecting the ancient with the hyper-modern. As McAndrew reminds us, "The essence of effectiveness, as always [will be] to locate a balance between technology and individuals."[1] Man, in twenty years and beyond, will still have the key role to play when it comes to fighting and winning wars.

In looking at the crucial issue of the future commander's information requirements, it will be necessary to explore and sketch out some preliminary outlines of the conditions of 2020. There is little point in trying to 'get it right' down to the very last detail; what is helpful is a set of parameters that help add shape and texture to the time just beyond the horizon. After a general landscape has been painted, it will be necessary to underscore the particular challenges that will face the next generation of army leadership. Some of the issues will be old and unchanged; others will see a shift in their relative importance.

The next part of the analysis is the tricky bit—trying to suggest what kinds of technological remedies might exist to overcome the obstacles delineated. The difficulty arises from the fact that the entire process can be rather self-serving. It would be too easy (and not very instructive) to construct challenges with certain technological fixes in mind. Conversely, there is a temptation in these kinds of crystal ball exercises to not only 'think outside the box', but to relegate 'the box' to the dustbin and describe an enchanted menagerie of technological *wunderkind*, some of which would solve all our problems, being omnipotent as well as omniscient. It seems to me, though, that while this kind of fancy does have utility in stretching our imaginations and leaving no stone unturned in the pursuit of 'the next big thing', it must be circumscribed in some way. Besides, the works of science fiction have proven to be most prescient in this regard, and to delve into that realm is not my aim. This trepidation rests on one simple premise: if, in precisely describing some future gadget, an error is made, and by some (great) chance, it does not come to pass as dreamt, any analysis that follows on from it loses credibility. Far better to put in place some general features that will characterize the technology of tomorrow and use those as the landmarks by which the contingent commentary can be judged.

Following on from this general description of the technological toolchest of 2020, it will be possible to delve more deeply into the areas that will require the most attention

now and tomorrow. An understanding of how much the future commander will come to rely on systems will be required. No army, from now on, will be able to act under the illusion that operations, theirs or those of others, can succeed if they are envisioned or conducted in a piecemeal manner. Whereas military history to date has produced advances in *combination-based* warfare (examples of which would include all-arms cooperation, joint doctrine, and notions of combined or coalition operations), the future must be centred on the concept of *integrated* operations. For the purposes of this discussion, an examination of C^4ISTAR will reveal the large differences that exist between these perspectives.

Finally, as opposed to positing wild and fantastic bits of hardware, this paper will include suggested courses of action to overcome the problems associated with moving from the current paradigm to the next; paradigms, as I have stressed, which are marked more by human activity and capability, than by any amount of high-tech 'boffinry'.

The Landscape

NATO (and most of its members) has offered two visions of the future, each based on a particular view of the potential threats that will present themselves. These views, while not necessarily expressed as such, should be seen as ideal types, caricatures of what might be the case. The differences between the views are exaggerated, and the subtleties and nuances are left out. They are stark pictures, useful in illustrating the extremes of the situations; nonetheless, they allow us to focus our thinking on what we might expect to encounter.

NATO's View 1 is based on the nation-state, and supposes several scenarios that might lead the Alliance to meet with what the Americans call a 'near-competitor'. Essentially, this view sees Western militaries up against an 'Iraq' or a 'Serbia', a state-based military with fairly modern and well-maintained Soviet-era equipment. These foes may or may not have weapons of mass destruction, but the clash with them is seen as largely conventional, with clearly defined theatres and battlefields. In this view the land force commander's information requirements would largely be the same as they are today: the intent of the enemy, his disposition and locations, etc.

View 2, often seen as a catch-all, a kind of insurance policy against View 1, envisages the greatest threats appearing from non-state or sub-state actors, whether they are warlords in some civil war setting, or international terrorists. Clearly, this view is gaining currency. The land force commander's information requirements would be much more difficult to define and would entail a series of challenges in their fulfilment.

The Challenges

By 2020, with the advances we can expect to see in 'conventional' adversaries as well as the rise of the international sub-state actor, the process of acquiring information to satisfy a ground commander's requirements will be a frustrating and seemingly never ending process. This will be due in part to the nature of the 'targets'. They will undergo

an evolution that will be the result of changes not only in technology, but also in economics, politics, and social relations. Whatever the causes, the result will be vexing on commanders and will test the abilities of the entire intelligence gathering apparatus.

Western commanders will not have to concern themselves with the comings and goings of large formations of men and equipment; the targets of 2020 will be smaller than those we have become accustomed to in the last 60 years. In View 1, they will take the form of single vehicles or platforms, with the capacity of a brigade of today, and the firepower of a Second World War division. In View 2, targets will continue to be based on cells, not motor rifle divisions. They will be clan or tribally based, with numbers in any one geography less than 200.

Not only will sizes be diminished, the clear lines between 'combatant' and 'non-combatant' will be blurred. In both Views, the garrison fence will be a less than helpful marker as to 'who is who' in the enemy camp. A reduction in size will mean that forces can blend into the societies that host them. The presence of women, children, and mercenaries will make target identification difficult, and the risk of failure more acute. As peace support operations have shown over the last decade, the notion of 'front lines' is increasingly losing currency. Especially in View 2 scenarios, international tourists, students, and migrant workers—groups which are set to increase throughout the West—will prove to be difficult contexts from within which targets will need to rapidly and accurately identified.

Conventional forces will continue the centuries old trend towards increased speed. Helicopters, drones, and lighter armoured vehicles will mean that static 'map overlays' and periodic documentary reports will not be able keep up with dynamics of the battle. The day of the paper INTREP is over.[2] 'Snapshot' reports will be next to useless as the commander finds himself almost constantly in motion, engaging with a series of moving and rapidly changing targets.

Size, definition, and speed will mean that targets—conventional or otherwise—will be dispersed, not over grid squares as they are now, but over whole geographies and regions, on land, over water, and throughout the air into space. The ideal of 'concentrating the effect and not the troops' will be more easily achieved, increasing the difficulty of predicting the location of the enemy, or his next attack.

This dispersion will drive, and be further driven by, the ability for forces to network themselves; that is, to connect and link their capabilities. Adopting the characteristics of other networks, the enemy of 2020 will rely less and less on any single part of the whole, and come to have ready built protection through redundancy. While this networked nature is nothing new in the world of View 2, it will come to be the standard in top-flight View 1 adversaries.

For the most part, the changes listed above will be compounded by the reality that wars will not be fought on battlefields anymore. It will not be possible to understand conflict in terms of one or two dimensions, taking place in strict linear time order. Map

sheets and overlays will not be able to represent campaigns that are being conducted in a variety of means, using several methods. Even the innovative US Marine concept of the 'Three Block War' falls short of describing the diversity of activity that will take place. To continue the analogy, more than city blocks, each house and building will represent a multitude of ambiguous factors that commanders will need to understand in order to conduct operations effectively. Frighteningly, from the perspective of someone who has the responsibility to 'know' the entire battlefield, some suggest an almost boundless future:

> The tactical battlespace will be multi-dimensional, stretching from the sub-surface environment to space. In physical terms, it will include all aspects of the space to sub-surface continuum, including the electromagnetic spectrum. It will likely be non-linear and potentially non-contiguous. The battlespace of the future will be the whole of time and space related to a particular operation.[3]

One of the greatest frustrations of the domestic police forces in the West has been the fact that criminals always seem to possess the initiative; policing, with a few exceptions, is largely a reactive activity. The same can be said for future security and military operations. The global system of governance is based, and will continue to be based for the foreseeable future, on the principle of inviolate state sovereignty, at least in the first instance. Countries like Serbia, for instance, are left to their own devices until after one (or more likely, a series) of violations of human rights or international law. The international community will not support 'active' methods of policing; Western militaries are not free to conduct pre-emptive strikes without at least a modicum of justification, and even then, this is reserved only for incidents that point to grave dangers. These dangers are usually the product of long periods of development (in the case of biological or chemical weapons production, for instance). Moreover, the targets of this kind of 'proactive' policing are generally pariah states (Iraq and Libya have been good examples in the past). The events in Afghanistan, and the deliberations over what the next stage in the campaign might be, are a testament to the 'respect' for sovereignty that underpins the international system. Intervention is not a decision taken lightly, and 'just cause' must be proven. Even so, it could be argued that the 'first move' still rests with the rogue or enemy; the decision to engage in nuclear weapons or missile development lies with the 'criminal' rather than the 'police'. This reactivity will mean that intelligence gathering and target definition will have to be done in extremely covert and non-intrusive ways.

One of the key problems with the NATO Views is that they tend to polarise our perspective and force to see things as either/or propositions. However, one of the most significant challenges likely to face militaries in 2020 and beyond is a combination of both View 1 and View 2; a synthesis of the dialectical points of view. For instance, we may see a state adversary employing both 'conventional' and terrorist tactics simultaneously, tending to confuse our efforts in gathering information and deter us from obtaining an accurate picture of what is actually happening. Seemingly separate events may well be connected; for example, a conventional attack on Western interests by a state may be preceded by a terrorist strike. On the other hand, events that appear linked may prove to have nothing in common at all, leading the West to overreact and make costly

errors. The synthetic nature of future threats and conflicts—the seamless transition and combination of Views 1 and 2—poses the greatest challenge to military forces in the next half century.

The Technology

As indicated in the introduction above, it is not my intention to describe fantastic gadgets and high technology solutions to the threats and challenges enumerated. Instead, a set of technological parameters will be posited; whatever the specific forms of weapons or sensors that are in service in 2020 and beyond they will share these broad characteristics.

More or less, given the heightened attention given to defence budgets in the wake of September 11th, whatever kind of technology is desired will be available by 2020. No sector of research and development will find itself unaffected by the events of New York and Washington, and the subsequent operations in Afghanistan and elsewhere. Information systems, biotechnology, 'smart weaponry': these will all experience a renaissance marked by increased interest and funding. The result will be that in twenty years, if it is wanted, and the resources are allocated to its development, it will be available.

Whatever the specific invention, in the fields of information gathering, we can rest assured it will be smaller than its forebears. Ideas of 'nanotechnology', with insect sized sensors, are already well developed. Weapons systems, too, will pack more punch in a smaller package; warheads and attack helicopters being two prime examples. Even in terms of military formations, we can expect them to be smaller and more agile. The Medium Weight brigade 'transformation' project in the US and Donald Rumsfeld's desire to reduce the size and number of the army division are precursors of this trend.

At the same time, technological advances will mean that our forces and systems are faster than those of today. Computing processing will definitely be faster; aircraft, armoured vehicles, and communications will all be accelerated. This speed, when combined with reductions in size, will mean that we are more agile, more easily deployed and repositioned.

Assets that are used by military commanders will have to be extremely adaptable, allowing them to be used in both View 1 and View 2 scenarios. There will not be a bottomless purse, so the need for 'more bang for the buck' will continue. Dual role (and dual use) platforms might be shared by intelligence agencies, security forces, and the military, especially in countries other than the US. Flexibility will remain a key characteristic in the future.

A virtue of any future military will be its ability to reach further than it can today. Tactical and strategic airlift, attack aviation, unmanned sensors, ground based weapons systems, and radio communications will all have extended ranges. The advent of space-based weapons will mean 'the death of distance'; nothing is out of range to a satellite.

This will mean that for Western militaries, just as for our opponents, we will be able to focus on the 'terminal effects' of our efforts, concentrating the capabilities of our sensors and weapons, without similar 'bunchings' of troops and equipment.

While it will be true to say that 'what we want we will get' (in terms of new technologies) the landscape of 2020 will also feature some of the same pieces of equipment in service today. Much of the remainder will have been designed in the 1980's and 1990's; the stuff of today's production 'pipeline'. In other words, not everything will be shiny and new. Just as today old and new systems will coexist, the future will be an amalgam of 'cutting edge' and 'last generation' technologies. The effect will be that pure solutions will not be entirely possible. The reasons for this hodge-podge are largely economic; capital project life spans will not be scrapped, even in the looser budgets post-September 11th.

Old and new platforms will find themselves a part networks; some pieces will be components of several networks simultaneously. To be sure, information will flow more easily between the functions of 'find' 'fix' and 'strike'. Information pathways will exist to facilitate established patterns of information sharing and commanders will be able to 'plug into' these networks to extract vital snapshots of intelligence and situational awareness. Recent work in the United States (most evidently displayed in both the National and Joint Readiness Training Centers) has proven the ability to equip every soldier in a brigade with GPS transponder, giving headquarters an instant and up-to-date picture of the disposition of its troops. Each platform will become a node within a system rather than merely a component of a military machine.

This 'netcentric' will have both positive and negative effects. Information flows will be faster and potentially more efficient, and the effects of several assets will be coordinated to a degree never before possible. However, there are indications that "applying these technologies increases the complexity of the battlefield and thereby increases the likelihood of chaotic behaviour, all of which increases confusion."[4]

Platforms that are now envisaged as sensors may well acquire the ability to 'fix' or 'strike' as well as 'find', but the more significant change will come in the form of weapons platforms collecting and transmitting information. The current idea of 'all-source' intelligence will be raised to a new level. From the rifle sight to the cruise missile, weapons will prove as valuable as sources of information as they are instruments of kinetic force. This is where the real effect of networking will be felt. This information (from number one rifleman's thermal sight, say) will be instantly collated and fitted into the larger picture, made up from composite data from the whole range of sensors and weapons. In fact, "in physical and conceptual terms, modern armies [will] no longer [be] organising around weapons systems, but rather around knowledge."[5]

That being the case, information collection is in itself a desirable activity. While of course it is not an endstate (information collection exists only to make further action possible), in the preliminary or critical stages of a battle of campaign, information gathering may take primacy over execution. 'Finding' may well prove to be more

valuable than 'striking'. This will have several effects. The first is that it will be vital to have the right assets deployed in the right areas. A soldier in a trench with a pair of binoculars and some means of communication (it may be that the binoculars themselves are able to transmit the images they capture) could be more appropriate that an entire regiment of main battle tanks or a spy satellite.

Secondly, each platform will have to be viewed with its information potential in mind. For example, is a helicopter loitering over the horizon more effective as a missile platform or as a means of observing and directing the efforts of other weapons systems? Currently, these decisions are overlooked in a military context, except in cases of covert surveillance or reconnaissance. In the future, they will be paramount in all 'phases' of an operation. Whereas, "the traditional triad in land operations in the industrial age has centred on the relationship between firepower, protection, and mobility. Future armies will add a fourth dimension: information."[6]

This new appreciation of platforms will mean that we adopt a *capability focus* rather than one predicated on sheer numbers of troops or pieces of equipment. We will see that it is the capability that matters, rather than possession of a specific platform. This capability may require that several components work together; no one item may be able to provide the desired capability. Networking will increase in importance, as we are able to draw together outputs from a wide variety of sources. So-called 'end-to-end' solutions will be sought, rather than individual jig-saw pieces.

The Systems

What will this capability focus mean to the current way in which we work? Of course, we can say that even today (and for some time before now) modern militaries operate systems. For example, the components of a simple artillery mission, developed in its modern form during the First World War, need to be connected in a system: the supported arms commander, the observer and caller for fire, the command post, and the guns all must work in harmony in order for the mission to be successful. Complex solutions are calculated more and more with the aid of sophisticated and powerful computers. What is wrong with the current system that will let us down in the future?

In order that we might focus our attention and concentrate on a tangible system, I will use the concept of C4ISTAR as an example of a network that exists to fulfil a commander's requirements for information and to facilitate his communication needs.

The US Army likes to characterise its forces as a system of systems. This is an accurate portrayal of most modern Western militaries. What holds these organisations back is the fact that each sub-system is not operating optimally. The system of systems is negatively affected by its weakest links. In the above example, for instance, where we formed a network of sorts to accomplish a simple artillery mission, each component often works with and from a different understanding of the situation. The supported arm commander does not know (that is, he does not have perfect visibility) of the competing priorities of the artillery commander. The artillery commander on the other hand, must

rely on his network of observers; he cannot tap into other perspectives that may be better for the execution of the mission. Moreover, once the mission is fired, the target effects may well be reported and target data recorded, but to what extent is that information shared or made available to other interested parties? How long does the process take and how standardised is the process across arms or services? In peace support operations, there have been attempts to compile databases of information on events, incidents, and personalities in order that trends might be observed and better deployments attempted. Each has been frustrated by a lack of common information architecture.

In the context of C^4ISTAR, we can see each component system is not developed to the same extent. Remarkable advances in information systems technologies extant in the private sector are not equally evident in military communications or command and control, for instance. Something that works in one area cannot be guaranteed to be in use everywhere else. In certain cases, critical information cannot be shared easily across the entire network. If we look at surveillance and target acquisition, for example, we can see that very sophisticated equipment may be brought to bear in the collection and analysis of thermal and audio data, allowing detachments to form a clear picture of what is in front of them. But there is no way at present to transmit that information to the wide variety of potential users, other than by a radio message containing a crude interpretation, or a cumbersome process of video or audio capture and transmission of a tape, usually by runner or dispatch rider. We might want to assume that these glitches will be solved in the next twenty years, but it is not a certainty that they will. More fundamental and potentially dangerous hiccoughs have been allowed exist for longer periods of time; effective and reliable combat radios are not currently in service in all Western militaries, including that of the United Kingdom.

The key reason for this inequity is the way in which the systems were designed. C^4ISTAR began its life as C^2, or command and control; later STA (surveillance and target acquisition) were 'bolted on'. Each component piece experienced its own separate path of development, evolving in some instances using information technology as an impetus; in others, doctrine or experience forced improvements and 'upgrades'. C^4ISTAR, then, is the result of a series of conceptual additions; it is not a wholly independent concept in its own right.

This kind of thinking is characteristic of other military doctrines as well. Joint theory, as an example, has been the sum of individual service doctrines and capabilities, rather than an independent body of thought.[7] In short, military theories tend to be based on *combination*. They are usually designed 'bottom up' rather than 'top down'. At first, this approach may seem sensible, as it properly takes into account the specific qualities and strengths of each component and adds them together. However, this kind of cumulative thinking tends to prevent any real kind of synergy from being formed. Pfaff asserts that, "In fact, the more subsystems there are and the more coupling between them the more likely chaos is."[8] If we were to design C^4ISTAR as a desired endstate, rather than a clump of capabilities, new directions and possibilities could be envisaged. By starting with a clean slate, the intrinsic weaknesses and 'bad habits' of each piece of the puzzle could be avoided. Symbolically, it could be said that currently militaries think in

terms of 'C+C+C+C+I+S+T+A+R' and in the future, they will have to think like 'CxCxCxCxIxSxTxAxR'.

This 'top down' approach is especially necessary when we are looking to design a network. Bolting together separate components, and then trying to form some kind of network around the resulting system entails a large degree of reverse engineering and 'cobbling'. If instead the network were envisaged in its entirety, and the individual components designed with the totality in mind, less jury rigging and work-arounds would be required. This perspective would be an example of true *integration* based thinking and exceeds the capabilities of combined solutions.

The Problems

What are the particular issues that militaries face, then, in trying to achieve integrated solutions? There are several, and although we are looking to the future, they have their roots in the present and the past. None are insurmountable, but each takes a significant shift in thinking to solve.

When we see the acronym C^4ISTAR we tend to think of it as a group of equal activities, each with its own unique but similar set of conditions and parameters. Others might see the alphabet soup as steps in a process (albeit not in any logical or terribly useful order). These perspectives are fine up to a point, but caution must be exercised in equating each piece of this conceptual daisy chain. The first 'C'—command—must be at all times seen as both the starting point and the necessary conclusion of any process. It alone can guarantee action. It, when properly carried out, can make up for enormous deficits in almost all the other categories. It can be supported and made easier through technological innovations, but it *can and should not be replaced* by any sort of mechanised or computerised surrogate. It represents the very soul of the network and the system and brings to the process of military operation the necessary human element. It is fragile and easily overwhelmed, but it is vitally important. No matter how great the advance, the temptation to allow any of the other functions overshadow command—be it control or target acquisition or intelligence—must be guarded against. "The challenge for the future commander will be to take advantage of [the technology] and to ensure that the human, and not the automated system, makes the final decision."[9] As we will see, the effectiveness of any C^4ISTAR concept relies on command in the first and last instance.

Currently a great deal of effort and resource goes into the research, design, development, and fielding of individual weapon and sensor platforms. The latest technologies in remote sensing and microtisation are brought to bear in the creation of innovative military hardware. However, due to the conceptual understanding that the military tends to exhibit (that is, to look at things in a 'bottom up' way) these individual platforms often outpace the systems required to properly integrate them into a coherent and effective network. The entire C4ISTAR process has been developed vertically (resulting in several freestanding 'silos' or 'stovepipes') and not horizontally, which would have seen interconnectedness as a primary concern. In effect, the 'pointy end' is miles ahead of the 'back office' and as a result, the full effects of the technologies cannot

be realised. Hardware developers ensure that their products can be 'plugged in' to existing systems, but they are often unaware of the possibilities for synergy that exist. As one field commander notes, C4ISTAR "gives us the collection, analysis, and collation capability; now can technology and doctrine give us the tools to achieve synergy among the various collection means?"[10] This 'horse before the cart' situation often arises because the military has not conceived of the need for synergy early enough and has not fully expressed the requirement to designers and producers.

What must change between now and 2020 is the way in which hardware is designed and delivered. As mentioned above, a clear comprehensive picture must be available showing the interconnectedness of the entire network, and the capabilities required, rather than individual bits and pieces, should be procured. The network must be present in the design, rather than being seen as an afterthought, or even as a final touch.

If we see this kind of integration and systemisation, the military will need to be cognisant of the kinds of information flows it is generating. Again, command here will be critical. Commanders are caught between asking for information to fulfil identified requirements (and thus being limited by their own experience or imagination) and being 'fed through a fire hose', becoming inundated with bits and pieces of information that, by virtue of their sheer volume, lose meaning. As Travers puts it, "Even though we are faced with information overload from high-tech sensors which provide an abundance of information on enemy dispositions, we still will not know an enemy commander's intent."[11] Already it is possible to 'micromanage' through 'overgathering' of information; subordinate commanders must be given the freedom of action to command and control their own forces. Just because a commander can have a piece of information, does not mean that he should.

The flow of information, then, should be command driven. Caution is again needed to avoid using unprocessed or uncollated data. Not only can it be too detailed to be of any use, it can lead to a climate of paralysis by analysis. Even the most sophisticated C^4ISTAR system cannot remove all doubt or risk from a decision. We are tempted, though, to wait for more information. Just one more reconnaissance mission, or satellite pass and a commander could improve his picture (say one of 85% certainty) and improve it to one of 95 or even 99%. Unfortunately, technology may never be able to deliver this kind of assurance and the slippery slope of waiting for more information can mean slower decisions, the exact opposite of what a largely automated C4ISTAR system is meant to achieve.

Another aspect of the management of information is information sharing. It is vital to inform various levels of command with important, relevant, and timely news on the situations of enemy and friendly forces, on terrain and weather, and future intentions and contingencies. However, again balance is called for, lest info-sharing turn into info-burdening. Human judgement will still be needed in order to preserve the concept of 'need to know', not just from an operational security perspective, but also from the point of view of relieving the strain on subordinates.[12]

Another temptation is the one to 'make use of all the assets at the commander's disposal'. This, too, can have the effect of slowing down executive decisions. Obviously, a prudent corroboration of information from a variety of sources is key to good decisions, but exhausting an almost endless catalogue of sensors may not be the most suitable solution. Just because we can do something, does not mean that we should; commanders of the future must truly assign 'horses to courses' and not simply 'courses to horses'. Somewhere along the line, a commander must be willing to accept the risk inherent in the concept of 'reasonable sufficiency'. A lone soldier's voice report, or a streamed video from a remote surveillance device, may indeed be enough to allow a commander to decide and commit his forces to action. The necessary ingredient in this process of balancing information with risk is judgement, a very human quality that militaries have been doggedly developing for centuries. Technological advances can go a long way to improving judgement, but they cannot replace it.

The Solutions

If what has come before has been a litany of challenges and potential problems, what follows is a set of recommended solutions. While they are based on an analysis of the future postulated by many observers, they have their genesis in the world of today (or even yesterday). In fact, some of them may have the air of common sense or 'motherhood' about them; what *should* be fixed today, however, *must* be fixed tomorrow.

In terms of the solutions about to be suggested, some key pieces of nomenclature are important to get straight. For the purposes of this section of the paper, a system will be composed of a process (a standardised way of doing things; either a set of tactics, techniques, and procedures [TTPs] or established doctrine); an organisation (some defined body of personnel; the Army, Intelligence, or Security forces, for instance); and a network (the physical hardware that enables nodes [like weapons, sensors, people, or processors] to communicate (data, voice, visual images, etc.) Other, more general definitions of the word system (such as may have been used before now in this paper) will not be precise enough from this point forward. It is important to note that a system is not just information technology or computing hardware; it is made of people and the things they do, as well as the tools they use to do them.

With this in mind, the solution recommended is the proper integration of all systems. If we continue to restrict our discussions to C4ISTAR, this point can be made quite clearly. The processes, organisations, and networks involved in C4ISTAR must be conceived of holistically and organically. A holistic approach will consider each piece in relation to the overall effect desired. It will not allow alterations (or lack of alterations) in any one segment to constrain the remaining segments, and therefore, retard the entire system. By taking an organic point of view, it is possible to see each component of the system as interconnected and essential for the systems proper functioning. What an integrated perspective avoids is both the combination practices of the past and the 'runaway technology syndrome' that results in information overload.

An army operating in a true integrated manner will follow a simple manner of development. It will first identify the capabilities it needs to either counter the threats it believes to be pertinent or project is influence. Second, it will design a system to make those capabilities possible. This is will do by designing a set of processes and from a map of those processes, it will create an organisation to carry out those processes, altering current structures as necessary. Lastly, it will design the network solutions to allow all the pieces to work together. This sequence may seem simple, but because it begins with the overall effect in mind, it is focussed on producing *capability*, not just *forces*. Its simplicity will be a source of criticism from some—until they are asked to implement it, when they will come up with many reasons why it is too difficult by half.

Systems integration, then, might be seen as bringing all the components of a system into proper alignment. Properly conceived this alignment takes place throughout the sequence, as opposed to some retrograde afterthought.

The first step in the systems integration is to articulate some desired endstate, some level of capability that is sought. There are many ways in which this might occur, and largely they fall outside the scope of this paper. Each country, and indeed each agency, has its own bureaucratic model for policy formulation. Politics (international and domestic) and economics will often have more impact in the result than will sheer military or security 'necessity'. Regardless of those greater machinations, what is germane to this discussion is that any desired capability can be developed in one of two ways. It can be inclusively conceived, drawing upon input from the Forces, academics, and other interested parties[13] or it may be conceived of exclusively, thrust upon the Forces without consultation. This choice of capability development also pertains to how new equipment is designed and procured. Do the Forces include industry in the formulation of the 'capabilities after next' or are these kept secret and isolated from the advances made in the private sector? Are the personnel functionaries in the armed forces included in the discussions around future changes?

In a world of truly integrated systems, cooperation must exist at this level. Only by understanding (and in some limited sense, shaping) the vision of the future, can industry supply the forces with networks. Only with this clear and common view can recruiting, training, and education be adapted to support what is desired. Without this early and inclusive integration, systems are doomed to endless rounds of 'jury-rigging', trying to fit networks and organisations into place.

The next step, once a common picture of what is required has been established, is to craft the processes by which these objectives are achieved. Processes can include everything from large-scale procurement, to medical evacuation, to battlefield information gathering. These processes derive from the objectives and must be both flexible enough to allow for changes and rigorous enough to convey benefits of standardisation and economy of scale. The aim of process redesign is not to homogenise operations; rather it is to ensure that there are ways in which people can work to achieve specific goals. If an organisation does not know its processes, it is not truly effective.

And if the basis for any process becomes "that's the way we've always done it', it is likely that the process is not suited to the changed and changing objective.

Once the objectives have been mapped out, and the processes designed to enable their realisation, the proper organisation must be created around these processes. It is not enough to give new tasks to existing organisations, built out of old understandings and for requirements perhaps no longer necessary. It is not suggested that change must be made for change's sake, or that the every organisation is obsolete. What is necessary, though, is a comprehensive reassessment of the alignment of objectives, processes, and organisations. This stage of the sequence will be the most difficult for armed forces to achieve. Inertia, steeped in regimental pride and service rivalry, is a significant force to be overcome. Looking more widely, jealousies between the armed forces and other producers and consumers of intelligence serve to do the same thing: maintain, and even bolster, the status quo--especially when 'billets' and 'manning credits' are involved.

These recommendations may seem agreeable enough, but one of the first questions to be raised will be, 'Who is going do all this?' Currently, the army may have directorates of force development, of personnel, of 'future concepts', and of development and procurement. What it does not have is a single agency dedicated to holistic systems design, no agency charged with conceptual integration. Some efforts have been made in the field of procurement, but again, they are too late in the sequence of events to be anything but band-aids.

Broadly speaking, there needs to be an office of *joint capability development*. Notice this is not force development; that exists already, and while it will have a part to play in the larger picture, the future will require an office with integration (of the entire system) foremost in mind. Obviously, a great deal of effort will be required to create such a directorate: educated staff must be selected and prepared; inter-agency links must be established; expertise and personnel will need to be transferred from service staffs and schools. Most importantly, though, commanders must support, not only the office, but also the concept and practice of systems integration itself. This will not be easy, but the requirements of the future demand it.

> The militaries that meet with the greatest success in future armed conflict will be those which can undertake rapid organizational and conceptual adaptation. Successful state militaries must institutionalise procedures for what might be called 'strategic entrepreneurship'—the ability to rapidly identify and understand significant changes in the strategic environment and form appropriate organisations and concepts.[14]

This integrated approach has not been the forte of militaries to date. Their histories and the demands of operations often work to create less than perfect solutions. In some areas, (such as heavy logistics, for example) this has given birth to the introduction of new players on the battlefield and in the halls of power. Alternate service delivery and consulting have reached new levels in several defence ministries. A particular case could be made for the inclusion of such experts in the systems integration field. Looking at the Bowman Radio Replacement project, it is easy to see that there

exists a need for someone to bridge the gap between the military's statement of requirements and industries production. Industry has tried on many occasions to perform this intermediary function itself (to no positive effect) and militaries, as it has been said, have tried to change their procurement processes accordingly.

Perhaps professional systems integrators are needed to perform this function. While certainly not the only players that could work in this space, they bring several qualities to the table. First, because of their industry knowledge—both wide (that is, spanning several sectors, such as communications and manufacturing) and deep (having worked within the industry's front and back offices and all along the supply chains) they bring a level of understanding of 'what is possible' beyond what a serving officer or official could. They see the best practices and they are involved in shaping the developments in several dynamic and relevant industry areas. This allows them to identify gaps in existing technological solutions, and enables them to advise on best of breed options. Furthermore, because they work with several agencies and firms, they can have a positive effect in bringing together like-minded organisations into partnerships. This both fulfils and creates opportunities. The militaries of tomorrow will need to have this breadth and depth if they are to operationalise their various, demanding capabilities.

If the true potential of these systems integrators is to be realised, then a mere external role will not be enough. Once more, since systems integration is possible only when a holistic approach is adopted, bringing systems integrators into the picture from the outset is critical. This allows them to provide their most valuable services, services that private firms rely on them for most heavily. System integrators can add tremendous value in the creation and validation of objectives in the first instance. While they should neither drive the process, nor replace all military input, they can inject what they have learned about the various industries in which they work. For example, if a certain capability the military is looking to acquire relies on improved communication, a systems integrator could provide insight into a full range of options, from wireless to fibre-optic solutions, including ideas about timelines and firms working in this area. This information can help shape decisions, early on, rather than waiting for disappointing tender proposals that necessitate a rewrite of the entire plan. Once an objective has been created, they are able to leverage their knowledge of industry best practices to suggest refinements to processes and organisational structures. If the integrators are seen as full partners in this way, they will provide not only invaluable insights into the industrial landscape, but also aid in the efficient design of the systems themselves.

The Conclusions

All of this may seem miles away from the land force commander's world in 2020. However, as it must be understood, the means of information collection and analysis do not arise from a vacuum. The very essence of any future success will be the extent to which a commander is connected with the tools to do his job. Old notions of service interests and specific-to-arm skills will need to be replaced with ideas that hinge on 'big picture' thinking and knowledge management. Furthermore, the results desire in 2020

will mean investments today; education and organisational redesign, for example, take time and resources to be effective.

Technology will be a critical component of the army of 2020 and beyond, but more important will be the way in which that technology is harnessed. Buying new gadgets of the shelf and 'shoe-horning' or 'bolting' them into existing networks will provide less than optimal outcomes. Integrating systems through a holistic conceptualisation involving a capability focus, an understanding of robust processes, and the will to form strong and relevant teams is the best way to ensure that the commander of 2020 gets what he wants, when he wants it. Harnessing the value of professional systems integrators and bringing them in early allows for opportunities to be identified and options explored from the start. Assistance in the creation and validation of objectives are valuable services that should not be overlooked.

The answer to the opening question, "How will we know?" may never be completely satisfactory. Uncertainty and the need for human judgement in decision-making will always exist. However, an integrated system taking information, technology, and people into account is the best way to ensure success for the future.

References:

[1] McAndrew, B. 1999. Soldiers and Technology. *Army Training and Doctrine Bulletin*. 2.2: p. 24.
[2]Travers, D. 2001. Brigade ISTAR Operations. *Army Training and Doctrine Bulletin*. 3.4/4.1: p. 49.
[3]Directorate of Land Strategic Concepts. 2001. Future Army Capabilities. *DLSC Report 01/01*. p. 7.
[4]Pfaff, C.A. 2000. Chaos, Complexity and the Battlefield. *Military Review*. Jul-Aug: p. 83.
[5] DLSC, p. 8.
[6] DLSC, p 8.
[7] See Ankersen, C.P. 1998. A Little Bit Joint: Component Commands—Seams Not Synergy. *Joint Force Quarterly*. Spring: pp. 116-121.
[8] Pfaff, p. 84.
[9] DLSC, p 18.
[10] Nordick, G.W. 2001. Exploiting Opportunity. *Army Doctrine and Training Bulletin.* 3.4/4/1: p 2.
[11] Travers, p. 45.
[12] Travers warns against the tendency to horde information when he says, "The mentality that [the retention of] information is power must be disposed of to ensure the continuity of effort required by intelligence and operations is seamless in its transition, and timely in its decision making. Intelligence is useless if it is not disseminated and it becomes detrimental to the operation if it is not disseminated in a timely manner." Travers, p. 48. However, this needs to be balanced with the advice from the DLSC: "All relevant data, information and knowledge must be available at all levels, but managed in a way that produces a current, rapid and coherent understanding of the battlespace, while at the same

time allowing the various levels of command to process the relevant material for their purposes." DLSC, p. 21.

[13] This is similar to the way in which the recent SDR was conducted.

[14] Metz, S. 2000. *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*. Carlisle, PA: USAWC, SSI. p. xv.