POINTER MONOGRAPH No. 2

Realising Integrated Knowledge-based Command and Control

Transforming the SAF

Jacqueline Lee
Melvyn Ong
Ravinder Singh
Andy Tay
Yeoh Lean Weng
John J. Garstka
Edward A. Smith, Jr.

Published by
POINTER, Journal of the Singapore Armed Forces
SAFTI Military Institute
500 Upper Jurong Road
Singapore 638364
website: www.mindef.gov.sg/safti/pointer

First published in 2003

Body text set in 11/14 point Garamond Book

Produced by
BOOKSMITH *consultancy*

Contents

DISCLAIMER

The opinions and views expressed in this monograph are the authors' own and do not necessarily reflect the official views of the Ministry of Defence.

About the Authors

CPT JACQUELINE LEE is an officer in the IKC2 SPO and believes that the future SAF officer must be conversant in both technology and operations domains. As the SAF enters the Knowledge Age, it is the synergy between both domains that will give us the competitive edge. She holds a B.Sc. in Materials Science and Engineering and a B.A. in Economics from the University of California, Berkeley.

CPT MELVYN ONG is currently a staff officer in the IKC2 Special Project Office and has played an active part in the conceptualisation and promulgation of IKC2 in the SAF since the inception of the SPO. He believes that military innovation is an ongoing imperative for the SAF and feels the process of experimentation will be crucial not only in realising tenets of IKC2 but also in the transformation of mindsets in meeting future challenges. It is the knowledge within our people that will be our sustainable edge. He holds a B.Sc. (Hons.) in Economics and an M.Sc. in Development Studies from the London School of Economics.

COL RAVINDER SINGH is currently Head of the Joint Communications and Information Systems Department (JCISD) in Joint Staff, MINDEF. COL Ravinder is a key proponent of Network-centric Warfare in the SAF and, together with the IKC2 Special

Project Office, has been instrumental in the leadership of the SAF's transformation efforts through Integrated Knowledge-based Command and Control.

He holds a B.A. (Hons. 1st Class) in engineering science from the University of Oxford and an M.Sc. in Management from the Massachusetts Institute of Technology. He is also concurrently the Deputy Chief Information Officer for the SAF. Prior to his appointment as Hd JCISD, COL Ravinder has also held various appointments in the Army such as ACGS (Plans), Comd 2 SIB and Dy ACGS(Ops). He had also spent some time in Kuwait as a UNIKOM Observer in the immediate aftermath of the Gulf War in 1991.

MAJ ANDY TAY has been a staff officer in the IKC2 Special Project Office since its inception. He believes that IKC2 will transform the way the SAF goes about its business. He feels that technology is only an enabler for transformation. It is the hearts and minds of our people that will go a long way in helping to realise IKC2 and various other transformation initiatives in the SAF. He holds a B.Eng. (Hons.) in Naval Architecture and Ocean Engineering from University College London.

DR. YEOH LEAN WENG is the Deputy Director (Command, Control & Intelligence) and Deputy Director (Communications), S&C4 of the Defence Science & Technology Agency. He joined MINDEF in 1983 after graduation from the National University of Singapore. Dr. Yeoh holds a B.Eng. (Hons.), three Masters in Communications Engineering and a Ph.D. in Electrical Engineering. He is currently an Adjunct Professor in Temasek Systems Defence Institute, National University of Singapore.

JOHN J. GARSTKA is the Assistant Director, Concepts and Operations, Office of Force Transformation and a recognised thought leader in the area of Network-centric Warfare. He is a recognised international speaker and has delivered the Network-centric Warfare message to military and commercial audiences worldwide.

Prior to joining the Office of Force Transformation, Mr. Garstka was the Chief Technology Officer in the Joint Staff Directorate for Command, Control, Computer and Communications (C4) Systems. In this capacity, he had played a key role in the development and conceptualisation of network-centric warfare and was the Joint Staff lead for the Department of Defense's Report to Congress on Network-centric Warfare.

DR. EDWARD A. SMITH, JR. is a retired U.S. Navy Captain with 30 years of service. He holds a B.A. in International Relations from Ohio State University and an M.A. and Doctorate in International Relations from the American University.

He saw combat in Vietnam as the Intelligence Officer on the staff of the Commander of U.S. Naval Forces in the Mekong Delta, completing almost 200 combat air missions in helicopters and OV-10 Broncos. Other assignments included duty in the Navy Field Operational Intelligence Office and in the Defense Intelligence Agency as Executive Assistant to the Political Advisor to CINCLANT/SACLANT, and as Assistant Naval Attache to Paris. He has also served as Assistant Chief of Staff for Intelligence for Cruiser Destroyer Group Eight in Battle Force U.S. Sixth Fleet. He was a primary player in creating the seminal U.S. Navy white paper "…From the Sea". His final tour in the Navy was on the personal staff of the Chief of Naval Operations where he directed the Navy's RMA war games and was the author of the U.S. Navy's *Anytime, Anywhere* vision. He retired from the Navy in 1998 and is now Boeing's Senior Analyst for Network and Effects-based Operations.

IKC2

Transforming the SAF in the Information Age

A Foreword by Chief of Defence Force

INTRODUCTION

Over the last three years, the framework for the capability development in the SAF has been based on Force Readiness, Force Evolution and Force Transformation.

Force Readiness

In the area of Force Readiness, we have to constantly reshape the SAF to be ready and capable of conducting a spectrum of operations.

For instance, the setting up of the Island Defence HQ is timely as it provides a multi-agency approach to homeland security. With September 11 and the more recent Bali bombing, the role of the SAF in homeland defence has just been further reaffirmed. Our participation in U.N. Peace Keeping Operation is another significant part of this reshaping.

By and large, we have responded to the Force Readiness requirements in the last few years within the context of an expanded spectrum of operations.

Force Evolution

Force Evolution is something that we are all familiar with. Today, we have a system in place for us to systematically develop the capabilities of the SAF within the current conceptual and doctrinal framework. Although the acquisition and phasing in of new platforms are challenging tasks, they are nonetheless known challenges. In this respect, the SAF can take these challenges in our stride.

Force Transformation

Force Transformation, however, is quite a different matter. Enhancing our capabilities based on the present framework will eventually bring us to a point of diminishing returns and we have to start seeding the next S curve, even as we continue to move up the present one. In our context, transformation is not only about introducing new technologies, but a more fundamental conceptual and doctrinal change. Hence, we have put in place a broad framework to realise transformation through creating the capacity for the conceptual study, experimentation and also to map out the transition plans. One aspect of transformation resides in the area of Integrated Knowledge-based Command and Control, or IKC2, which is the focus of this monograph.

WHY IKC2 FOR FORCE TRANSFORMATION?

There are three reasons why we have decided to focus on IKC2 as a key component of our transformation efforts in the SAF.

Advances in Info-Comms Technologies

The first derives from observations on how operations were conducted during the Gulf War in 1991, the Kosovo campaign in 1999 and the recent Ops Enduring Freedom in Afghanistan. Advances in Info-Comms Technology (ICT) represent the feasible space, the possibilities beyond which are even more exciting and, indeed, will represent a quantum change from how we conduct operations today. These are essentially new operational concepts enabled by significant advances in ICT.

Declining Cost of ICT

The second is that of the economics of investment in ICT. Unlike the cost of labour or other resources, the cost of computing power is plunging. For example, one calculation shows that relative to the price of labour, processing power has become cheaper by a factor of 5 x 10^{-12} or by a factor of 5 trillion over ten years.

Building on our People Advantage

The third reason for us is the nature of the SAF. Given that we are a National Service Armed Forces and relatively small, we must always shape our forces to capitalise on technology and draw on the innate strength of our people. Today, our youth are bred on a diet of the Internet and are experts at computer games. Therefore, it only makes sense for us to exploit this competitive advantage of our people.

SO WHAT IS IKC2?

I have no intention on delving too deeply on the subject of IKC2 as subsequent presentations in this monograph will give you more details. Instead, let me take a step back and spend a few minutes to elaborate on the name, IKC2.

Command and Control

Firstly, I am referring to a process when I speak about “Command and Control”. It is a process that begins with the gathering of information on our own forces and on the enemy’s, as well as information of other factors such as the local population and organisations, weather and terrain. Having gathered the information, we need to process the information, make an appreciation of the situation, identify the objectives to be achieved and formulate different courses of action to achieve them. We then have to decide on a course of action. Following which, we engage in detailed planning and issue orders through the appropriate means. The execution of the plan is then closely monitored by means of a feedback system so that the entire process becomes a continuous cycle.

Hence, Command and Control is as much about the technology and processes that enable it as it is about the commanders and staff who are an integral part of it. It is also clearly evident that Command and Control is a significant force multiplier. The faster and more precise our command and control are relative to that of our opponent, the more we will be able to dislocate him. What is required here is the need for us to create superior sensor capabilities. At the same time, our command and control system must be networked to the extent that information flows will not only be responsive but, for specific requirements, will also be able to cut through the organisational hierarchy, such as in a direct link between a sensor and a shooter.

INTEGRATED SYSTEMS FOR INTEGRATED WARFARE

Secondly, I refer to the term "Integrated". As many of you may know, we promulgated the operational strategy of Integrated Warfare in 1994. Our thinking behind Integrated Warfare is quite a fundamental one. The underlying logic is that the bigger the optimising universe, the more optimal the solution. In the case of an SAF organised largely along Service lines, it was important to engender the mindset that regardless which Service was developing the plan, they should plan on the basis of the entire SAF's capabilities and not just those within their own Service. An integrated solution also creates more problems for our adversaries as there is a greater range of possibilities that they would have to prepare for. Therefore, the chance for tactical and operational surprise is enhanced. To realise Integrated Warfare, one basic requirement is the integration of our command and control system across the whole SAF.

NETWORK-ENABLED AND KNOWLEDGE-BASED

The third term is “Knowledge-based”. This is not a new phenomena although it is certainly a New Economy term. In the Old Economy, SOPs are knowledge made explicit, disseminated so that staff can be trained to apply them efficiently and effectively. In the context of IKC2, tacit knowledge will again be made explicit, but it is embedded in decision support systems and software agents. This will ease the load placed on the commanders and staff so that they can focus more on values and judgement-based issues and less on technical analyses and decisions. In a networked command and control environment, a knowledge-based approach is also good economics as the network provides the multiplier effect.

THE ROAD AHEAD

Now that we know the “why” and the “what” of IKC2, what are some of the challenges ahead for the SAF as we seek to integrate IKC2 into our capabilities? Our culture is obviously one of the big issues but I do not intend to address that. Instead, let me touch briefly on three specific issues that would have to take culture into account.

SHORT-TERM PAIN VS. LONG-TERM GAIN

The first is an inter-temporal issue—that of short-term pain vs. long-term gain. IKC2, by identifying the flow of information within and between Services, will enable the streamlining and sharing of C2 resources across the SAF. However, the implementation of IKC2 in the SAF may cause some initial delay in the more immediate C4IT programmes. Master-planning will therefore be needed to reduce the duplication of software programmes and projects that can cut across Services. Initially, adherence to standards and requirements stipulated under the IKC2 framework will possibly slow down the current pace at which individual systems and capabilities are fielded. However, this will potentially yield enormous capability benefits as a result of the effective interoperability and long-term cost savings due to the reusability of common modules. Implementation of subsequent C2 systems will also be much faster than today once the core part of the architecture has been established.

A more important inter-temporal trade-off is between investing in Force Readiness and Evolution vis-a-vis that of Force Transformation. How much should we invest in IKC2 in order for us to adequately prepare for the future? What percentage of our defence budget should go into Force Transformation? There is no correct answer to these questions. At best, we can only put in place a framework for us to take reference from. What is clear though is the need for us to create a dedicated bandwidth to address Force Transformation issues. Otherwise, the urgent issues will always displace the long-term ones.

Platform vs. C2

The second area is that of the trade-off between platforms against that of C2 systems. Notably, our budget is always finite and we have to prioritise our investments. The cost of ICT investments are falling very rapidly. We will therefore have to review our plans with regards to acquiring platforms and, perhaps, even how we train and operate.

Reviewing of C2

The third area is that of our present command and control structure and organisation. Technology only provides the means. We must change how we organise and operate. The traditional reliance on hierarchical models for information fusion and decision-making must therefore be replaced by networked structures for greater flexibility, lateral connectivity and collaboration across organisational boundaries. These are complex issues and they must be examined from the point of what is most optimal for the SAF. It is clear that more options must be explored while recognising that it is not optimal for the SAF to operate on a hierarchical model that fails to optimise the increased speed of command and control that IKC2 potentially offers.

CONCLUSION

The possibilities with IKC2 are tremendous. It is a journey that will lead us_towards a stronger SAF that is able to deal effectively with threats across the entire spectrum of conflict.

I hope you enjoy this monograph.

LG LIM CHUAN POH
CHIEF OF DEFENCE FORCE

1

IKC2 FOR THE SAF

ORGANISING AROUND KNOWLEDGE

COL Ravinder Singh, MAJ Andy Tay,
CPT Melvyn Ong & CPT Jacqueline Lee

INTRODUCTION

Today, an information-led Revolution in Military Affairs (RMA) is upon us. Advancements in communications, sensors, information and precision-strike technologies, as well as the rapid proliferation of information networks such as the Internet, are creating a qualitative change in the information environment. When synergised with improved tactics, training and procedures, this technology trend will facilitate system-of-systems capabilities that will allow our armed forces to jump the next war-fighting capability S-curve. As current war-fighting platforms approach decreasing returns in terms of performance and affordability, the concomitant fall in prices of Info-comms technologies in particular mean that an information-led transformation is increasingly realisable for the SAF.

The information-led RMA will basically allow us do these things faster and better with an order of magnitude difference. How did this revolution come about? After all, networks of communication are not new to the battlefield. For example, radios and even computer nets have been and still remain part and parcel of our current capabilities. But today, it is all about "networks". Networks of sensors are able to capture and process huge quantities of data, networks of shooters are linked throughout the theatre and networks of information brimful of data race back and forth through our command structures. It is with this in mind that the SAF should embrace the Integrated Knowledge-based Command and Control (IKC2) framework to leverage on these information advances and better effect the Integrated Warfare doctrine.

DEFINING IKC2

IKC2 is essentially network-enabled and knowledge-based. It builds on the comparative advantage of the SAF in its techno-savvy people, technologically superior forces and a systems approach. As such, it is a force multiplier that will enable us to do more with less through the overlapping of sensors, shooters and communication nets across the entire battlespace.

WHAT IS IKC2?

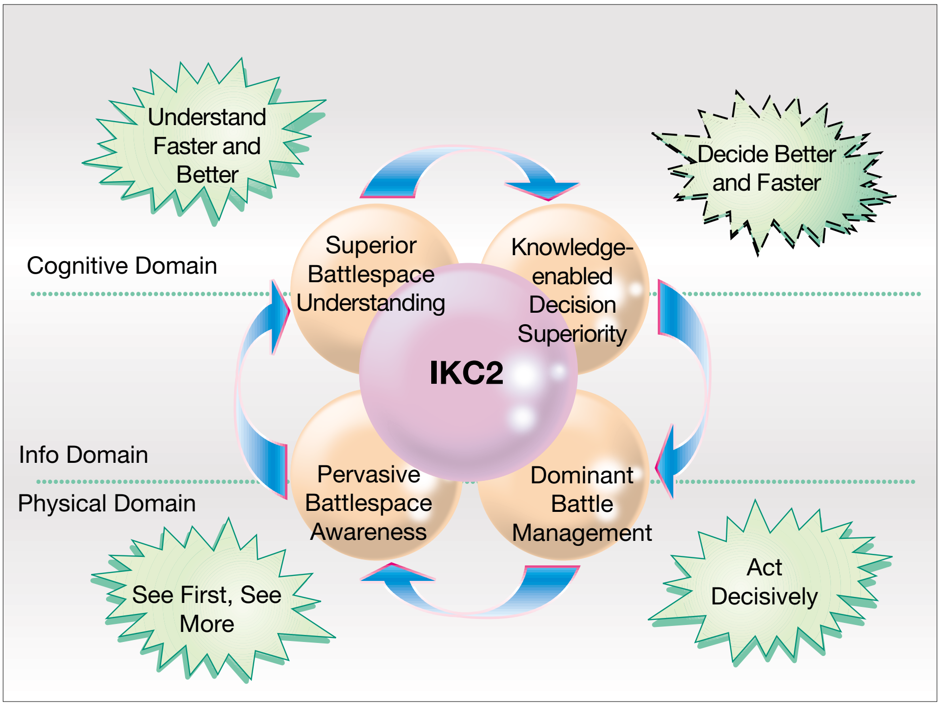
INTEGRATED WARFARE

NETWORK-ENABLED

ORGANISING AROUND KNOWLEDGE

FOR EFFECTIVE COMMAND AND CONTROL

IKC2 is conceptualised as network-enabled, knowledge-based war-fighting that is predicated on the OODA loop. "Observing", "Orienting", "Deciding" and "Acting" are essential components of any war-fighting cycle from the way information is assimilated, decisions made and actions taken. IKC2 therefore aims to exploit C4IT technologies to ensure that not only does one's OODA operate faster than the adversary's, but also that we are able to effectively disrupt the adversary's OODA cycle.


Understand Faster and Better
Decide Better and Faster
Cognitive Domain
Superior Battlespace Understanding
Knowledge-enabled Decision Superiority
IKC2
Info Domain
Physical Domain
Pervasive Battlespace Awareness
Dominant Battle Management
See First, See More
Act Decisively

In the physical domain, we want to see first and see more through Data and Information Superiority. In the cognitive domain, we want to understand faster and better and attain Knowledge Superiority. We also want to be able to decide better and faster for Decision Superiority. Finally, we want to be able to act faster and more decisively in order to achieve Effects Superiority.

In IKC2 parlance, we will strive to achieve all this with Pervasive Battlespace Awareness (PBA), Superior Battlespace Understanding (SBU), Knowledge-enabled Decision Superiority (KeDS) and, finally, Dominant Battle Management (DBM).

PERVASIVE BATTLESPACE AWARENESS

PBA is the entry pre-requisite for the SAF's vision of IKC2. It refers to the collection of relevant battlespace data by both operational and intelligence sensor entities, to the fusion of this sensor data into information. Imagine a sensor and information web that networks all sources of information: visual sightings, radar surveillance data, unmanned ground sensor signals, UAV pictures, acoustic surveillance pictures, satellite imagery, electronic intelligence data, communications intelligence, and so on. This network will provide powerful, persistent and pervasive coverage of the battlespace that is also innately robust as all sensors operate as part of a netted whole. The networking of sensor resources will therefore enhance the shared situational awareness among forces at all levels, across all Services.

SUPERIOR BATTLESPACE UNDERSTANDING

The key objective of SBU is to give commanders and decision-makers an effective understanding of the battlespace, with links to past knowledge and contextualised information. The idea here is that all war-fighters will have access to all data, information and knowledge that reside in a large library or warehouse in the network. The information is therefore available "Anytime, Anywhere and to Anyone". Intelligent fusion and correlation of these inputs also mean that war-fighters will receive the information that they need to make a decision, and not be subjected to information overload. Imagine a knowledge and semantic web that overlays the sensor and information web and provides the user with contextualised, ready-to-use knowledge about the battlefield. This will help commanders arrive at a better and quicker appreciation of their own forces and the enemy's intent.

KNOWLEDGE-ENABLED DECISION SUPERIORITY

KeDS follows on from SBU and involves automated, intelligent agents or decision support systems that support a commander's decision-making by analysing and proposing creative options for mission planning. Imagine decision support agents that are able to automatically analyse the complexities of the battlefield, monitor the progress of operations and postulate mission outcomes. This will help commanders reach better decisions, quicker.

Dominant Battle Management

The derivation and dissemination of clear commanders' intent will enable subordinate commanders to understand their mission and exercise full initiative in performing their tasks. This will culminate in the self-synchronisation of forces. Imagine the ability to employ firepower, move logistics replenishments and deploy reserves based on a just-in-time principle with full cognisance of the battlefield. Imagine the added ability to dynamically task and re-task weapons and aircraft while not having to wait for a new strike planning cycle should target priorities change. Imagine the ability to create precise weapon effects with perfect weapon-target matches with in-depth knowledge of the target. Co-operative engagement capabilities also mean that we may be able to launch an air force weapon against a navy target from the data and knowledge acquired from an army ground sensor because we are all operating on the same grid. All these will fuel our DBM capabilities.

POSSIBILITIES FOR IKC2

The possibilities with IKC2 are endless and depend on how we are able to innovatively exploit technology in our war-fighting processes. IKC2 has the potential to multiply our war-fighting capabilities.

The U.S. Navy conducted an experiment pitting F-15Cs fitted with the Joint Tactical Distribution Information System (JTIDS) in dogfights against those with only voice communications. The results showed that the kill factor more than doubled for a network-centric force[1]. In Millennium

[1] Source: JTIDS Operational Special Project – Report to Congress, December 1997

Challenge 2002, a Joint netted fire experiment by the U.S. Marines showed that networked forces could consistently overcome forces three times their size.

New War-fighting Concepts

IKC2 endows the SAF with many possibilities for furthering Integrated Warfare. Within the domains of PBA, SBU, KeDS and DBM, IKC2 will allow the SAF to operationalise a myriad of knowledge-based war-fighting concepts that are part of a matrix of capabilities for effects-based operations. These include capabilities such as the Strategic Sensor Web, Theatre-Wide Precision Strike (TW-PS), Cooperative Engagement Capabilities (CEC) and Just-in-Time Automated Logistics, to name a few.

Flatter C2 Structures and Effective Forces

IKC2 will also enable the SAF to achieve greater force optimisation through the networking and sharing of tri-Service assets to better achieve mission and targeting requirements across Service lines. It will also contribute to a more flexible and flatter C2 structure. Through the ability of forces to self-synchronise their actions, there is greater flexibility and efficiency of action. At the tactical level, this may result in rapidly configurable, deployable and survivable, mobile and lethal forces that are able to operate autonomously within a netted environment across the spectrum of operations.

Speed and Quality of Decision-making

In terms of decision-making, IKC2 will enhance the quality of decisions through the new knowledge that is created through collaboration in the information domain. This incipiently reduces uncertainty in the battlefield and gives rise to better decisions. The speed of decision-making also increases, enabling a higher tempo of operations to be effected.

Implementation Strategy for IKC2

To realise all this, we need both a "top-down" strategy and governance to build the enterprise communications architecture essential to achieve a system of systems. A "bottom-up" experimentation approach will complement this as the Services conceptualise and experiment with knowledge-based, network-enabled war-fighting in the various battle labs and experimentation centres.

CONCLUSION

The SAF IKC2 framework posits a network-enabled, knowledge-driven command and control concept for Integrated Warfare. With technological advances fuelling improvements in information reach and quality, the IKC2 framework is fundamental towards better utilising this knowledge for integrated SAF operations. This involves a parallel review and integration of our business processes and technology development, whereby a co-evolution of our doctrines, organisational structures, war-fighting concepts and technological innovation is needed for exploiting the info-enabled RMA. It is only through such a holistic approach to IKC2 that the SAF can be transformed, thereby providing a sustainable edge in this Knowledge Age.

2

ACHIEVING IKC2

AN ENTERPRISE ARCHITECTURE APPROACH TO C2 DEVELOPMENT

Dr. Yeoh Lean Weng, DD(C2I), S&C4-DSTA

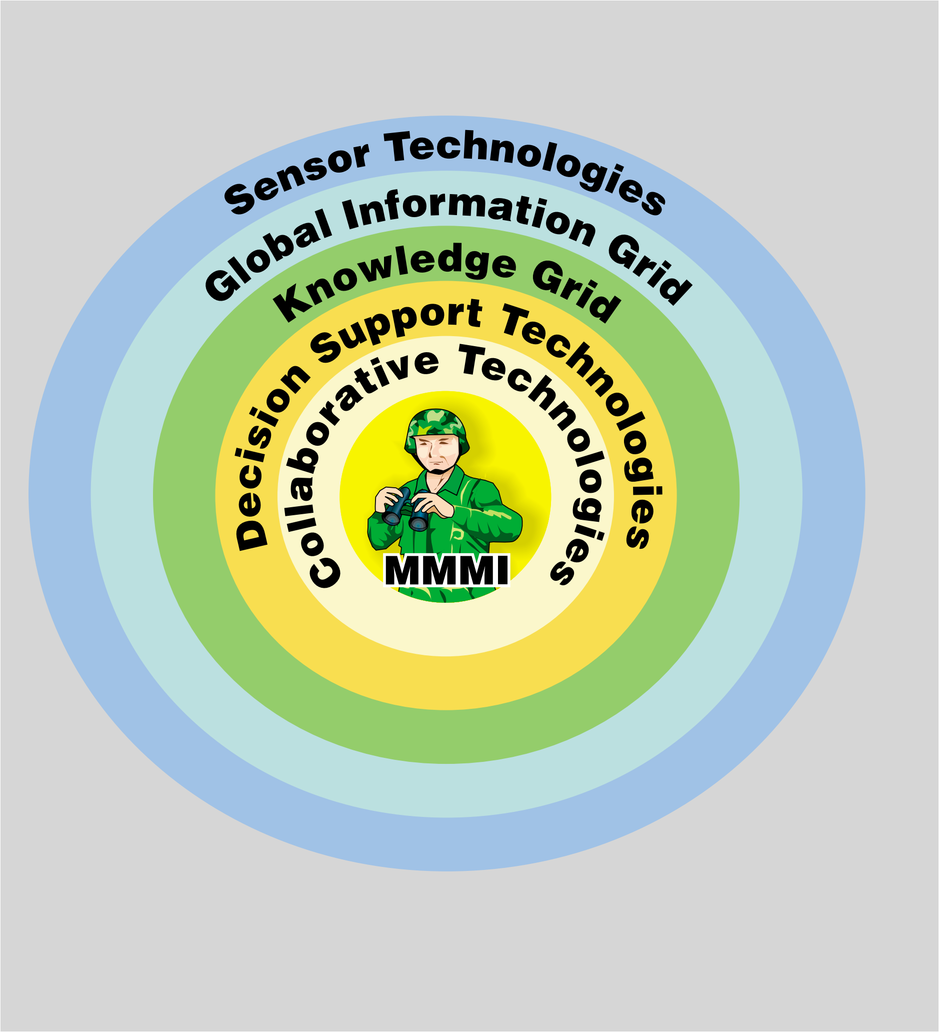
INTRODUCTION

Now that the concepts of IKC2 have been clearly articulated in the last chapter. The next step is to develop an enterprise architecture approach as a technological stepping stone in our journey towards an operational reality for IKC2.

OODA LOOP AND C2

For each state of the OODA loop, the supporting technologies can be represented in a framework centred round the commander as the main decision-maker. Such a framework consists of several components, namely, the sensors, a Global Information Grid, a parallel Knowledge Grid, service providers and interfaces with the intended users.

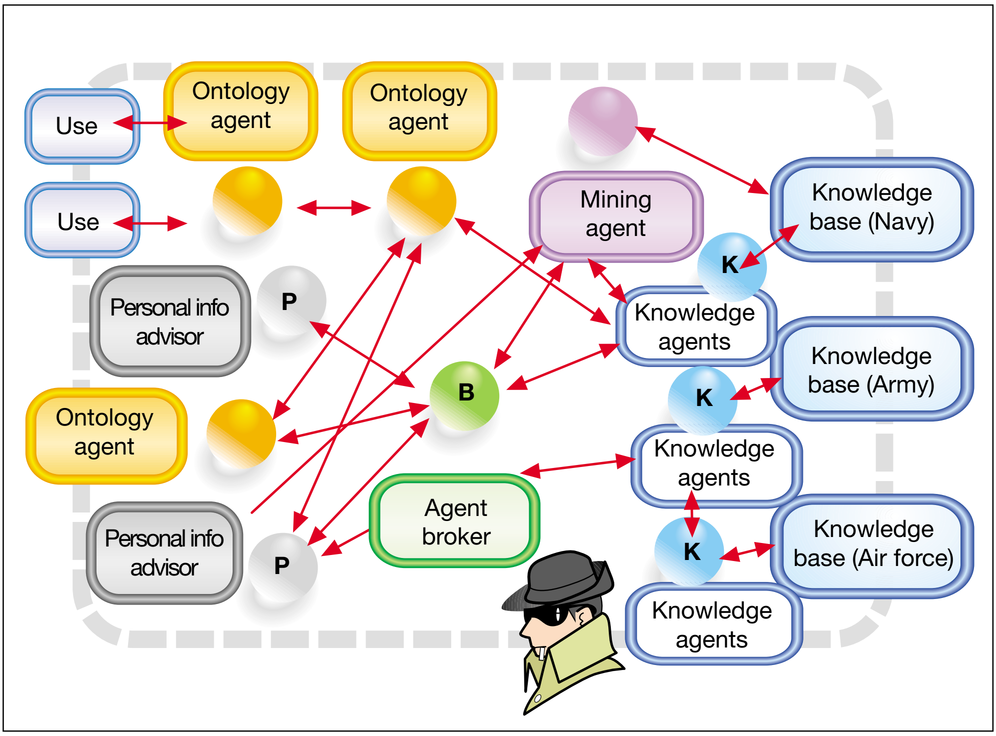
Sensors are the eyes and ears of the war-fighters. Information from a host of different sources can be fused together using a suite of intelligent data fusion algorithms to form a consistent battlefield picture for heightened situational awareness. The Global Information Grid consists of a network of communication nodes that move data and information from information sources to commanders. Also, in a service-based architecture, all information sources can function as service providers specialising in key demand areas such as terrain, own forces, weather and intelligence. Subsequently, the Knowledge Grid transforms information, so that it can be interpreted in the right context to produce knowledge.

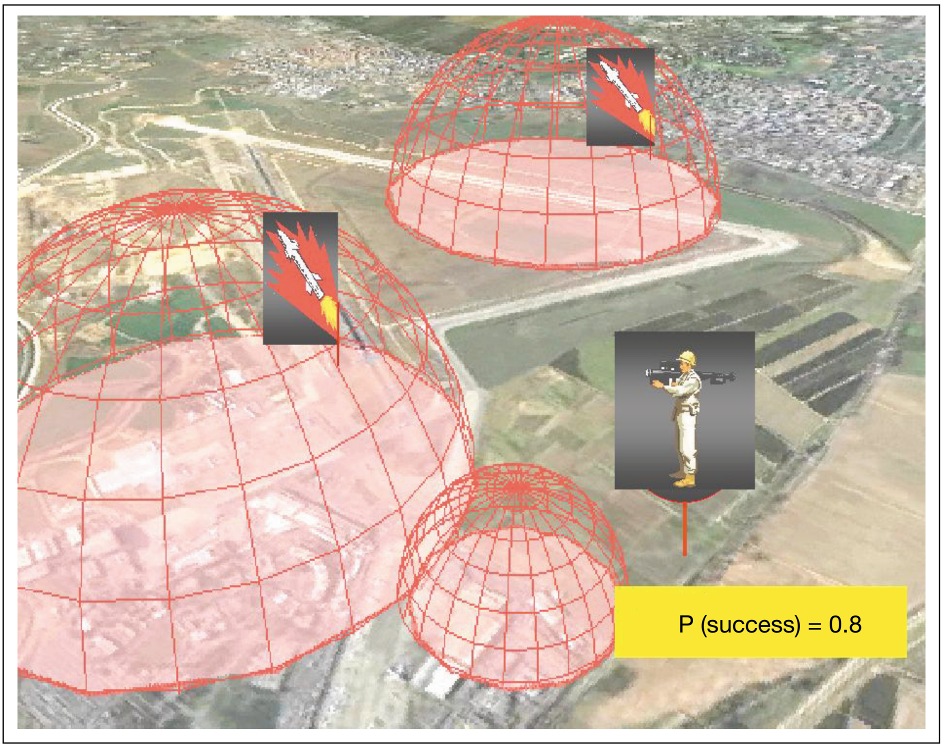


INFORMATION AND KNOWLEDGE

How then can we ensure that information is interpreted in the appropriate context for different users? First, we can create a common knowledge base layer to encode explicit knowledge with an ontology that classifies common terms. This is the essence of an information architecture where definition of terms must be precise among different users. We call this the semantic web.

With a knowledge grid, intelligent software agents can interact among themselves and negotiate with the various service providers to derive ECAs and OCAs based on the knowledge acquired. A commander can plan his mission with the help of decision support tools and collaborate with both higher echelons and lower subordinates within a multi-agent info-brokering environment.



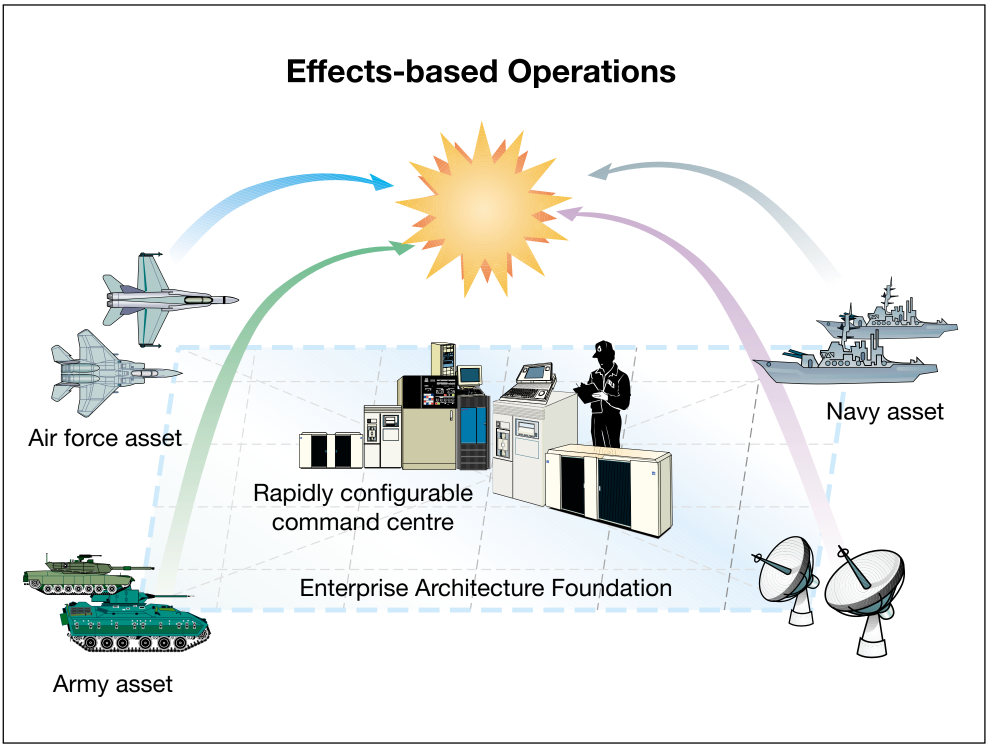


Collaboration is key towards the sharing of ideas, with virtual teams working on situational assessment and problem-solving across geographic and temporal boundaries. Today there are tools that use video conferencing, chat-rooms and white-board sharing, assisting them to make quality decisions. Once these plans are derived, they are evaluated through realistic, high resolution embedded war-gaming and simulation. With agent-based models and intelligent scenario generators, battle scenarios and possible courses of action based on specific goals defined by the commander can be generated. Commanders can use advanced simulation tools to evaluate the various options before he makes a final decision.

MAN-MAN-MACHINE INTERACTION

Man-man-machine interaction (MMMI) constitutes one of the most important components of a C2 system. It is the layer where the machine 'presents' knowledge to the commander to enable him to make critical decisions. Multi-modal interaction frameworks incorporating speech, gesture, handwriting recognition and symbol representation to derive a contextually appropriate interpretation are emerging today.

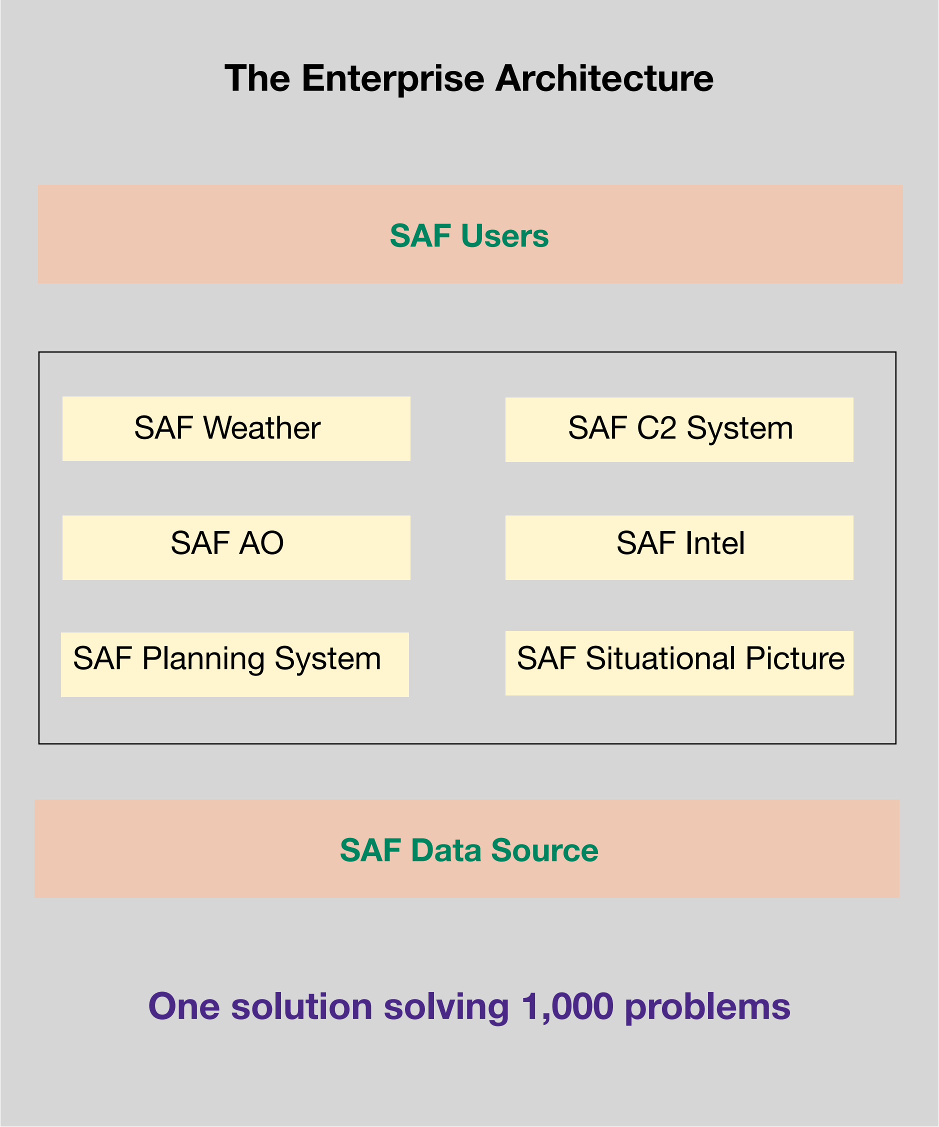
In this knowledge-centric environment, a Common Operational Picture (COP) provides commanders with consistent, contextualised graphical depictions of the battlespace. For example, an unidentified aircraft intruding into our air space need not be classified as hostile by the local air defence units. But if this aircraft is heading towards a naval task force, then it may be demarcated as hostile for a given ROE at a given point in time. The same information can be presented but different deductions can be drawn based on different operational contexts. Information with context creates knowledge. Such tools can help us improve on co-operative engagement concepts and sensor-shooter capabilities, as we move towards more effects-based operations in the future.


Effects-based Operations
Air force asset
Navy asset
Rapidly configurable command centre
Enterprise Architecture Foundation
Army asset

ENTERPRISE ARCHITECTURE

What then is an Enterprise Architecture? And how do the technology components fit into the architecture?

An Enterprise Architecture can be defined as “a strategic information asset base, which defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs”. Therefore, only one solution is needed to solve 1,000 problems, instead of having to conjure up 1,000 solutions for 1,000 problems.



The Enterprise Architecture

SAF Users

SAF Weather

SAF C2 System

SAF AO

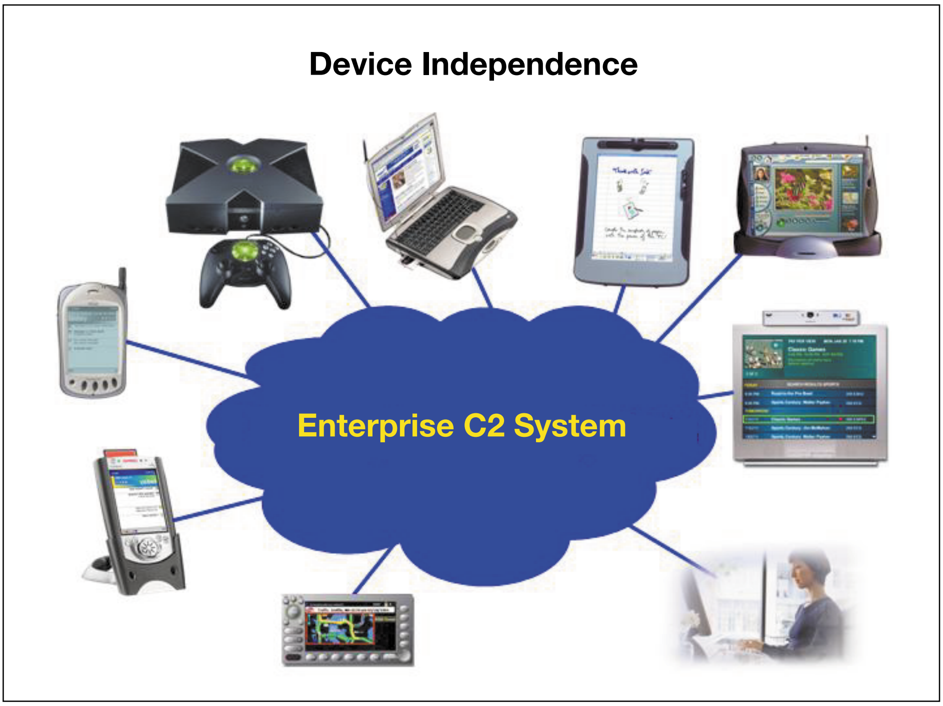
SAF Intel

SAF Planning System

SAF Situational Picture

SAF Data Source

One solution solving 1,000 problems



The Enterprise Architecture begins with a three-tiered architecture framework, with clean separation of the client, business logic and data layers. This further evolves when the middle tier expands into multi-tier layers. By doing this, scalability is improved because the components of the various layers can be changed without affecting the other layers.

The architecture is created with "plug and play" characteristics. It allows "device independence", so that there is no restriction on the types of applications and devices that can be "plugged" into the system. To illustrate how this integration-ready architecture can be developed, we start with a multi-tiered architecture for component scalability. Next, each application is treated as a "service" open to the whole enterprise by using a standard service description. This common protocol is called Web Service Definition

Language (WSDL). Next, a common transaction language between clients and between services is needed. This is called Simple Object Access Protocol (SOAP). After the services have been published, a directory of services for others to locate these services is needed. This is similar to the yellow pages and is called Universal Description Discovery and Integration (UDDI). Finally, transactions need to be managed to ensure that the service is rendered in a timely manner. (Application server frameworks such as Java to Platform Enterprise Edition, J2EE, and .NET will help to manage these transactions by dynamically allocating the computing resources as and when they are available to optimise the operations.)

SERVICES IN A MULTI-TIERED ARCHITECTURE

Putting the architecture into C2 perspective, clients are represented by the users and services are applications such as weather, terrain and intelligence.

The process to publish and subscribe to a service thus becomes very simple. The publisher creates the web service and defines a standard interface that others can recognise. He then registers the web service in the "yellow pages", for example, an SAF Directory of Services so that anyone who needs the service will know where he can find it. If anyone wishes to access the service, he looks for the service in these yellow pages and he can then access the web service directly in this multi-tiered architecture.

At the base, a service-based architecture allows seamless sharing of information. A semantic web placed upon the service–based architecture translates information to knowledge. Finally, decision support, collaboration, and Man-Man-Machine Interface (MMMI) technologies then effectively support the human cognitive loading. The end result is the SAF Command Control Information Systems (CCIS) sitting on the IKC2 framework that supports the OODA loop.

CONCLUSION

The technology challenges to build an enterprise C2 system are just the tip of the iceberg. Changing the mindset of our people will be the most challenging task. The success of IKC2 will depend on commanders like you, who dare to make the difference.

3

Military Innovation Through IKC2

Living in the Right Column

COL Ravinder Singh, MAJ Andy Tay,
CPT Melvyn Ong & CPT Jacqueline Lee

> "And it is worth noting that nothing is harder to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things."
>
> Nicollo Machiavelli

TRANSFORMATION TODAY

When Thomas Edison's electric light replaced oil and gaslights, it was transformation. When Henry Ford replaced the horse with the car as the common mode of transportation, it was transformation. Simply put, transformation is broad, sweeping and, most often, disruptive. It is the kind of change that affects the way we think, work, play and in our case, the way we fight. We have seen this many times before in the military. For example, when automatic weapons replaced single-shot rifles, when aircraft and armoured vehicles replaced wagons and horses. Today, precision strike rather than carpet bombing is *de rigeur*.

	Incremental – Traditional Missions	**Disruptive – New Missions**
Existing Technology	*Improvement – Fill in the Box*	*Recombinant Innovation – The capability to recombine existing elements in new ways*
New Technology	*Satisficing – Ruled by existing specs and mental models*	*Strategic Innovation – Key success factor is the ability to marry breakthrough technology and concepts*

RIGHT COLUMN

LIVING IN THE "RIGHT" COLUMN – THE INNOVATOR'S DREAM

It is the "Innovator's Dream" to have at his disposal the twin protagonists of new technology and disruptive concepts of war-fighting. Referring to the figure above, the attainment of strategic innovation is precisely the outcome of the ability to marry breakthrough technology and concepts.[1] In many of these cases of innovation, technological developments have clearly played an enabling or facilitating role in precipitating fundamentally new and more effective ways of fighting.

[1] This point was raised by John Kao (Chief Executive of Kao and Company) during a discussion with the Future Systems Directorate in February 2003.

Technology-driven Innovation

Prior to the 1980s, early technologies such as the telegraph, telephone and radio paved the way for other technologies such as the television, early generation computers and satellites that linked the world and the battlefield in ways that had never been seen before. The radar, for example, was used so successfully in World War II that Germany blamed the defeat of the Luftwaffe during the Battle of Britain on Britain's fighter control network. Other experts also argued that the evolution of sea warfare in World War II revolved around the radar since it aided planes in taking off from carriers and in their return. In other words, it was hugely instrumental in transforming carrier aviation. Computers provided individuals and organisations with a much greater capacity to collect, analyse and utilise information while satellites greatly expanded the global communications infrastructure. When these technologies synergised with breakthrough concepts, the recipe for strategic innovation was sown.

Several technologies stand out as part of the information revolution in the last two decades, such as smaller semiconductors, faster computers, fibre optics, cellular technology, satellite technology, the Internet, improved man-man-machine interface and digital compression, to name a few. Many of these technologies relate to advances in the realm of information-related capabilities and have expanded the soldier's ability to communicate.

IKC2 and Strategic Innovation

IKC2 is the SAF's overall framework for living at the edge of the IT-based RMA. It will leverage on advancements in sensors, communications, computing, information and precision strike technologies to develop war-fighting concepts that are network-enabled and knowledge-driven. This involves the transition of military forces from platform-centricity to a more knowledge-centric paradigm that will be the decisive war-fighting edge in the networked battlefield.

Today, the linking of near real-time information to PGMs through digital C2 systems has enabled more precise targeting that is more lethal and

The U.S. Army conducted a War-fighting Experiment (AWE) in 1997 to determine the effectiveness of a digitised division-sized force.[2] The Division wide area network that was 48 times faster was equipped with augmented network-supported additional applications such as video conferencing, and higher volume and faster data transfers as well as exchanging formatted messages, client-server operations and web-based operations.

The heightened battlespace clarity, increased situational awareness and information superiority over the OPFOR permitted the Experimental Force to conduct distributed, non-contiguous operations over the extended battlefield. The Division capabilities improved significantly.

- Quicker Planning: Div-level plan development time was reduced from 72 hours to 12 hours.
- Heightened Ops Tempo: Time required for processing calls for fire reduced from 3 minutes to 30 seconds, increasing responsiveness and lethality.
- Planning time for deliberate attacks at the company level was cut by half—from 40 to 20 minutes.

minimises collateral damage. Rapidly advancing sensor technologies are fast complementing advances in the lethality of PGMs. Sensor platforms, manned or unmanned, can now detect and track troop movements, individual vehicles, ships or aircraft well beyond the visual range, providing real-time targeting information for long-range engagement systems. The advent of cutting edge ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) technologies such as remote imaging satellites,

[2] D. Alberts, J. Garstka, R. Hayes and D. Signori, "Understanding Information Age Warfare" (September 2001), pp 259–261

optronics and synthetic aperture radars that penetrate cloud cover provide commanders with an unprecedented array of capabilities for the amassing of highly accurate information. When synergised with traditional C2 systems, all these contribute to automated sensor-to-shooter cycles that reduce the OODA decision time cycles. The resulting information advantage can be rather startling.

From a technology-centric perspective, our ability to operationalise and conceptualise disruptive ways of doing things through IKC2 will be critical to how we exist and thrive in the bottom right quadrant—that of strategic innovation.

IKC2 and Recombinant Innovation

However, IKC2 is not only a marriage of new technologies and disruptive concepts. At its most primal level, it is concerned with simply doing things better in a network-centric environment regardless of whether existing or new IT is enabling this innovation. After all, "to network" is a verb while "a platform" is a noun. In moving from platform to network-centricity, power forms whenever we shift from focusing on things to focusing on behaviour. In other words, the potential for innovation in a network-centric environment, be it recombinant or strategic, is, ironically, hugely predicated on the individual at the centre of this technology-concept divide. It is the thought and innovativeness of the individual that will determine our journey to the right column.

In fact, one of the most remarkable things to have come out of the current conflict in Afghanistan has been the integration of literally a nineteenth century military capability—the horse cavalry—with 50-year-old B-52s. This was integrated thanks to satellite technology and the innovativeness of its practitioners. Donald Rumsfeld, the U.S. Secretary of Defence, joked that the use of horses was all part of the U.S. transformation plan.

During World War II, the stunning effectiveness of the German campaign against France and the Low Countries in May 1940 was not simply a matter of the Wehrmacht possessing better tanks or having greater numbers. In fact, the Allies possessed a numerical edge of 1.3 to 1 in tanks, while many of their armoured fighting vehicles possessed superior protection and armament to German tanks. Moreover, at the outset of the May 1940 campaign, the Allies had force ratios of around 1.2 to 1 in manpower, a slight edge in Divisions (1.03 to 1) and from Luxembourg to the Swiss border, the French had completed the Maginot line.[3]

The Germans achieved through sound concepts for mobile, combined arms warfare and a well-trained army. In addition, German officer training had long emphasised initiative, risk-taking and leading from the front at all levels of command—in other words, the basic leadership principles for modern, mobile warfare.

Another piece of innovation witnessed in Afghanistan is the way young, non-commissioned officers were routinely integrating multiple intelligence collection platforms by simultaneously coordinating what many have called a "chat room". They were integrating real-time intelligence from the RIVET Joint surveillance aircraft and JSTARS as well as satellite information with SIGINT and Predator UAV inputs in a truly remarkable way. In fact, this "joy stick" generation displays an agility in doing things that comes clearly from being comfortable with new technology, a comfort developed from childhood.

[3] W. Murray and B. Watts, "Military Innovation in Peacetime" (June 1995), pp. 12–20

The BLU-82 bomb that was originally developed in the late 1950s for clearing helicopter landing zones (HLZs) in Vietnam became known as the "Commando Vault". However, U.S. forces in Afghanistan have used it in a new way—striking hard and deeply buried targets. On 9 December 2002, it was used on a cave near Tora Bora, Afghanistan, that was occupied by the Al-Qaeda leadership at the time. The cliff had originally posed a difficult challenge to U.S. planners because of its location and the large amount of rock covering. However, the massive pressure wave generated by the BLU-82 killed many of those inside the cave.[4]

Many of these innovations today involve changes in information-sharing capabilities and how they are being used creatively. For example, the JSTARS was designed to monitor static battlefields but has been used over Afghanistan to cue other platforms such as the Global Hawk which, in turn, cues other systems. This allows U.S. forces to conduct a wider search of the battlefield or what is termed "persistence over the battlefield".

What these examples demonstrate is that though technology is often a key enabler for new ways of doing things, transformation goes beyond technology, to the changing of mindsets and mental models. It is also a matter of changing our culture into a culture of innovation and intelligent risk-taking. We should not punish individuals for failure, and we also do not want to punish them for taking risks because risks will inevitably involve some possibility of failure. It is more important that individuals learn from their failures. Hence, this emphasis on intelligent risk-taking will be critical

[4] B. Bender, K. Burger and A. Koch, "Special Report: Afghanistan – First Lessons" in*Jane's Defence Weekly* Vol. 36 Issue 25 (19 December 2001)

towards how capabilities will be developed in a network-enabled, knowledge-based SAF. Within a networked environment, the commander becomes all the more significant in the way decisions are made and in the way concepts of war-fighting evolve.

EXPERIMENTATION – "WHAT IS THE QUESTION?"

Experimentation will be key towards capability realisation in IKC2. At one level, this culture of exploration must manifest itself in the way we frame our thoughts and derive concepts even as we frame the feasible space for experimentation. We need to "ask the right questions" rather than strive for answers that may well not answer our chief concerns. There are three ways in which this culture of innovation can be reached[5].

Innovation Begins With an "Eye"

One way is to observe events and actions around you and by simply being attuned to the information within the environment. Many questions will abound as to why many military processes and actions are what they are.

Prototyping is the Language of Innovation

Create as many physical or mental prototypes as you can and learn from the failure of each product or idea. In this case, communication, the flow of ideas between people and the process of enhancing one's understanding, becomes just as important as the final product itself.

Immersing in the Future

Constantly be aware and assimilate new ideas that are "in the market".

[5] Tom Kelley (General Manager, IDEO) presented this idea at the Island Forum in Singapore, 13 September 2002.

Predicated on this culture of innovation, the experimentation framework can be divided into three different layers that make up the systems approach towards capability development.

Technology Component Experiments

Such component experiments should focus on demonstrating the operational relevance of key technological tools such as intelligent decision support agents, modelling and simulation designs, mobile C2 networks, knowledge management tools and dynamic C2 systems among others.

Operational Component Experiments

These experiments would follow from the technology component experiments, further developing the work processes and operational procedures that complement the given technological tools. Designed around the IKC2 operational tenets of PBA, SBU, KeDS and DBM, such experiments add process and operational relevancy to the experimentation process.

Capability Demonstrations

Scenario-based and integrated capability demonstrations can showcase the nature of the capability area. The effectiveness of a capability area can be depicted within a specific scenario or even in an integrated-force setting, culminating previous developments in technologies, operational processes and organisational force structure changes.

To this end, we must adopt a “Dare to Dream and Dare to Do” spirit in experimentation. This not only involves being creative in adopting new technological solutions but, more importantly, changing our current mental models and work processes to fully exploit the potential of emerging technologies in designing innovative operational solutions. It is only through such a holistic approach to IKC2 that the SAF can be transformed, thereby providing a sustainable edge in this Knowledge Age.

CONCLUSION

IKC2 will change the way we think and the way we fight. However, we need to articulate disruptive concepts that will "take us to the right column" of strategic and recombinant innovation. Experimentation will help clarify the path we are to take. It will provoke us to ask, "What is the question?" Along the way, answers may be derived but more questions will inevitably surface. The very nature of IKC2 experimentation is that we should expect failure. Not that we set out to fail, but the whole thinking behind it is that we do not in fact know what all the risks are. Therefore, we are prepared for the possibility of failure knowing full well that we will learn from the experience, and that these minor blips are inconsequential to the larger organisation as a whole. There are two mindsets that we have to deal with here. One is from the leadership who must understand the nature of experimentation, and there is a leaning in the right direction. The second is from individuals involved who must not flinch from daring to experiment for fear of failures. We will have to put in place the appropriate conditions for such mindsets to change.

Once again, "to network" is a verb while "a platform" is a noun. In moving from platform to network-centricity, the innovativeness of the individual will take on even greater importance. Ultimately, the soldier will be at the heart of any military innovation.

4

Network-centric Warfare

Increased Combat Power for Joint Military Operations

John J. Garstka

(Adapted from an article of the same title published by the Office of Force Transformation, U.S. DoD, 2001)

Network-centric operations are military operations that are enabled by the networking of the force.[1] When these military operations take place in the context of warfare, the term network-centric warfare is applicable. Network-centric operations provide a force with access to a new, previously unreachable region of the information domain. The ability to operate in this region provides war-fighters with a new type of information advantage, an advantage broadly characterised by significantly improved capabilities for sharing and accessing information. By appropriate employment of tactics, techniques and procedures, war-fighters can leverage this information advantage to dramatically increase combat power. Across a broad spectrum of mission areas, evidence for the power of network-centric warfare is emerging from experiments and exercises. Evidence collected to date supports a strong correlation between information sharing, improved situational awareness, and significantly increased combat power. A common theme in this evidence is the critical role of modified (in some cases new) tactics, techniques and procedures in enabling war-fighters to effectively leverage an information advantage. The intent of this paper is threefold:

[1] VADM Arthur K. Cebrowski, USN, and John J. Garstka, "Network-centric Warfare: Its Origin and Future" in *Proceedings of the Naval Institute* 124:1 (January 1998), pp. 28–35

- to describe key aspects of network-centric warfare;
- to highlight evidence that demonstrates the power of network-centric warfare; and
- to address key implementation challenges.

WHAT IS THE INFORMATION DOMAIN?

The Information Domain is the domain where information lives. It is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information between war-fighters. It is the domain where the command and control of modern military forces is exercised, where the commander's intent is communicated. The potential scope or span of the war-fighter's information domain is defined by the state of information technology and the extent to which it has been deployed within a war-fighting force. The information domain is and has been ground zero in the battle for an information advantage—and as history notes—the cost of not having an information advantage in warfare can be high.

WHAT IS INFORMATION ADVANTAGE?

An information advantage is a condition in the information domain that is created when one competitor is able to establish a superior information position vis-à-vis an adversary. The concept of an information advantage is not new. Commanders have always sought—and sometimes gained—a decisive 7information advantage over their adversaries. Indeed, surprise, one of the immutable principles of war, can be viewed as a type of information advantage that one force is able to establish over another.

A relative information advantage can:

- be persistent or transitory;
- exist in some areas of the battlespace but not others;
- be measured in the context of a task or set of tasks;
- be created by taking actions to reduce our information needs and/or increase the information needs of an adversary; and

- be achieved through the synergistic conduct of information operations, information assurance, and information gain and exploitation.[2]

Information Superiority, as envisioned in the U.S. Military's Joint Vision 2020, can be interpreted as a relative information advantage of such magnitude that it results in a significant imbalance in the information domain. There is historic precedence of the impact that the possession of a relative information advantage can have in warfare.

During World War II, a key contributor to the success of Operation Overlord, the Allied invasion of Europe in June of 1944, was the ability of Allied forces to establish and maintain an information advantage at the operational level of war. The ability of the Allied intelligence apparatus to break German codes and keep Allied codes secure gave senior Allied commanders confidence that the vast deception operation that had preceded Operation Overlord had succeeded. Furthermore, at the time of the invasion, Allied forces were aware of the geographic positions of all but a few of the forty plus German Armies Divisions in and around the Normandy area that could be brought to bear to oppose the Allied invasion. This significant information advantage enabled the Allied invasion force to achieve surprise and a decisive force advantage on the beaches at Normandy. Nevertheless, at the tactical level, there were several instances during the invasion where Allied forces did not have an information advantage, where paratroopers were dropped in the wrong location and landing craft attacked the wrong beach.

Network-centric operations can provide a networked force with the capability to improve its information position and overcome limitations such as those that existed at the tactical level during Operation Overlord. They can allow a force to develop a new type of information advantage that can be leveraged to create increased combat power at the point of contact with an adversary.

[2] Office of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence), *Information Superiority: Making the Joint Vision Happen* (The Pentagon, Washington, D.C.: November 2000), available online at www.c3i.osd.mil/infosup/

WHAT IS A NETWORK-CENTRIC FORCE?

A network-centric force is effectively linked or networked. A network-centric force has the capability to share and exchange information among the geographically distributed elements of the force. It is possible to envision a fully interoperable force where information can be exchanged between sensors, regardless of platform; shooters, regardless of Service;

Network-centric Warfare

Translates an Information Advantage into a decisive War-fighting Advantage

Information Advantage – enabled by the robust networking of well-informed geographically dispersed forces

Characterised by:

- Information Sharing
- Shared Situational Awareness
- Knowledge of commander's intent

War-fighting Advantage – exploits behavioural change and a new doctrine to enable:

- Self-synchronisation
- Speed of command
- Increased combat power

Information Sharing is a Source of Combat Power!

and decision-makers and supporting organisations, regardless of location. However, it is important to note that a force with these capabilities is not known to currently exist in any of the U.S. Military Services or in the armed forces of any of our Allied or Coalition partners.

In the U.S. Armed Forces, there are sectors of each of the four Services that are robustly networked, where sensors and weapons can effectively exchange information. It is within these sectors that the information domain is being extended and evidence of the power of network-centric warfare is emerging.

NETWORKING THE FORCE: EXTENDING THE INFORMATION DOMAIN

The networking of the force changes the landscape of the war-fighters' information domain. It extends the existing domain and provides access to a new region, to a new operational envelope. This new operational envelope corresponds to the network-centric region of the information domain. Within this region reside information constructs that are enabled by the network, constructs such as the common operational picture and the common tactical picture.

Operating within the network-centric region of the information domain allows war-fighters to achieve an information position that was previously not feasible—to develop a type of information advantage that was previously not possible. Understanding this somewhat abstract concept is key to leveraging the power of the network to increase combat power.

EMERGING EVIDENCE FOR THE POWER OF NETWORK-CENTRIC WARFARE

The increased combat power that can be generated with network-centric operations has been demonstrated in a broad range of mission areas in service and combined experimentation, operational demonstrations and high-intensity conflict. A significant and growing body of data provides evidence that the following conditions are valid across a broad spectrum of mission areas.

Improved Information Position	$I_{nc}(t) > I_{pc}(t)$
Increased Shared Situational Awareness	$SSA_{nc}(t) > SSA_{pc}(t)$
Increased Operational Tempo	$OPTEMPO_{nc} > OPTEMPO_{pc}$
Increased Loss Exchange Ratio	$R_{nc} > R_{pc}$

(nc = network-centric, pc = platform-centric).[3]

Evidence supporting these conditions in mission areas of counter air, counter special operations forces (CSOF), and Theatre Air and Missile Defence (TAMD) are highlighted below.

A U.S. AIR FORCE OPERATIONAL SPECIAL PROJECT

Some of the most compelling evidence for the power of network-centric operations developed to date is provided by an Operational Special Project conducted by the U.S. Air Force to evaluate the military utility of tactical data links employed by F-15Cs. Data collected from more than 12,000 sorties and 19,000 flying hours demonstrated that the kill ratios for aircraft equipped with Joint Tactical Information Distribution System (JTIDS) over non-JTIDS-equipped adversaries were extremely high, increasing by over 2.5 times in offensive and defensive counter air missions.[4]

[3] John J. Garstka, "Network-centric Warfare: An Overview of Emerging Theory" in *PHALANX*, December 2000

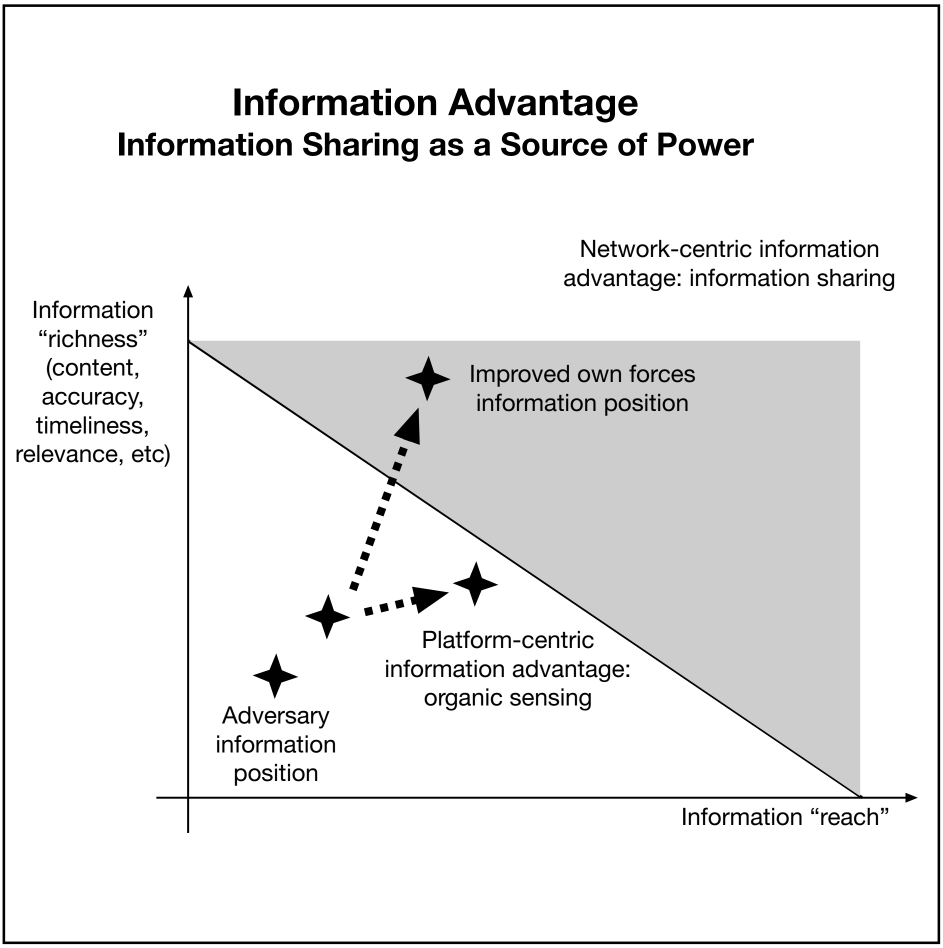
[4] JTIDS Operational Special Project (OSP) Report to Congress, December 1997, Mission Area Director for Information Dominance, Office of the Secretary of the Air Force for Acquisition, Headquarters U.S. Air Force, Washington, D.C.

The digitisation and networking of the F-15Cs enabled digital information to be shared between platforms, resulting in a significantly improved information position for the JTIDS-equipped F-15Cs. It is clear that when compared to the information position of fighters operating with voice-only that pilots flying F-15Cs with data-links were able to establish a relative information advantage that translated to a significantly higher level of shared situational awareness. The pilots were then able to exploit this advantage of awareness and employ innovative tactics, techniques and procedures to significantly increase their operational effectiveness.

FLEET BATTLE EXPERIMENT DELTA

Recent proof of the enormous power of shared information enabled by a network-centric force was provided by Fleet Battle Experiment (FBE) Delta, conducted in October 1998 in conjunction with Exercise Foal Eagle 1998, an annual joint and combined exercise sponsored by Combined Forces Command Korea. In this experiment, the seemingly intractable problem of countering hundreds of North Korean special operations boats, a counter special operations forces (CSOF) mission, was dealt with on a timeline previously not thought possible. The application of network-centric concepts enabled elements of the Army's 2nd Infantry Division, AH-64 Apache Squadrons, and a range of Navy and Marine Corps units to operate in the network-centric region of the information domain and to share a common operational picture. This resulted in a very high level of shared situational awareness that allowed these forces to employ new tactics, techniques and procedures that enabled them to synchronise their efforts from the bottom up. The net result was that a Joint and Combined force demonstrated the capability to dramatically increase combat power and to accomplish their mission in the half the time required for traditional platform-centric operations.[5]

[5] VADM Arthur K. Cebrowki, USN, written testimony to hearing on Defense Information Superiority and Information Assurance – Entering the 21st Century, held by the House Armed Services Committee, Subcommittee on Military Procurement, 23 February 1999


Information Advantage
Information Sharing as a Source of Power
Network-centric information advantage: information sharing
Information "richness" (content, accuracy, timeliness, relevance, etc)
Improved own forces information position
Platform-centric information advantage: organic sensing
Adversary information position
Information "reach"

THEATRE AIR AND MISSILE DEFENCE

In the Theatre Air and Missile Defence mission, the networking of sensors and shooters enables a force to significantly improve its war-fighting capability. In this mission, sensors play a key role in generating battlespace awareness. Stand-alone radar sensors, such as the E-2 Hawkeye, and sensors on weapons platforms, such as the AEGIS radar, detect and track objects ranging from aircraft to cruise missiles and ballistic missiles. When these sensors are employed in the operational environment in the stand-alone mode, scattering and environmental effects can combine to degrade detection and tracking capabilities, particularly against stressing targets (for example, high speed, low observables). This drop-off in operational performance can be manifested in poor track continuity, unacceptably slow track convergence or, in the worst case, the inability to initiate track.[6]

The networking of sensors enables a force to improve its information position by overcoming the limitations of sensors operating in stand-alone mode. The improved position in the information domain achieved with sensor networking in the U.S. Navy's Cooperative Engagement Capability (CEC) is portrayed in using the metrics of information richness and information reach. At the next level of fidelity, this information position can be characterised by increased track accuracy and identification (reduced uncertainty), as well as a decreased time required to achieve a fixed level of accuracy. An example of improved track accuracy vs. time representative of networked sensors tracking targets on ballistic trajectories is shown. In addition to being more accurate, this improved information position is less sensitive to environmental factors such as rain, which can degrade operational performance.

The improved information position enabled by the networking of sensors improves the war-fighter's capability to apply force and engage targets. It accomplishes this by facilitating the war-fighter's ability to make key decisions such as when to engage a target and which shooter/weapon combination maximises the probability of a kill. In addition, the ability of the force to share high quality information in near-real time has the potential to help a force employ new tactics, techniques and procedures such as "Fire on Remote Data", an approach which enables a shooter to engage a target with information provided by an external sensor.

[6] David S. Alberts, John J. Garstka and Frederick P. Stein, *Network-centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised)* (Washington, D.C.: CCRP Press, 1999), pp. 140–149

NETWORK-CENTRIC OPERATIONS: IMPLICATIONS FOR COMMANDERS

The ability to increase combat power at the tactical level provides operational commanders with increased flexibility to employ their forces to generate desired effects across the spectrum of operations. Emerging evidence shows that network-centric warfare can provide commanders with an improved capability for dictating the sequence of battle and the nature of engagements, controlling force ratios and rates of closure, and rapidly foreclosing enemy courses of action.

For example, consider the operational situation associated with a CSOF mission. If a Maritime Component Commander can dramatically increase combat power in the CSOF mission, then the Ground Component Commander has the option of reallocating his ground forces to other mission areas that he might otherwise need to keep in reserve to deal with SOF forces that penetrate defensive forces.

NETWORK-CENTRIC WARFARE: EMERGING INSIGHTS

NCW IS NON-INTUITIVE

One of the major insights that have emerged as a result of ongoing NCW initiatives is that the combat power associated with network-centric operations is non-intuitive. It is seldom possible for war-fighters to be able to identify new tactics, techniques and procedures that can be employed to leverage an information advantage before they actually experience and operate with an information advantage. In many situations, new tactics, techniques and procedures are developed only after war-fighters have had the opportunity to operate and train with an information advantage and develop confidence that the network that provides the advantage is dependable and can be trusted. Only after this stage is reached do new ideas that are the source of new tactics, techniques and procedure begin to emerge.

Importance of Experimentation

Networking the force is necessary but not sufficient for generating increased combat power. The non-intuitive nature of network-centric operations requires robust experimentation in the information domain. Robust experimentation is key to the development of new tactics, techniques and procedures that leverage the superior information position that can be achieved through networking the force. Experimentation can provide the hard facts that are required to build the case for investments that are required to network the force and address legacy interoperability problems. Getting the facts out is as important as getting the facts right. Without a widespread understanding of the power of network-centric operations, it is extremely difficult for military organisations to develop the traction necessary to allocate the resources required to robustly network a force.

Networking – A Key Component of Modernisation

Today's defence environment provides defence planners with a vast array of modernisation challenges. Historically, the focus of modernisation has been platform-centric. This approach has resulted in the deployment of a wide range of "advanced weapons systems" with systemic interoperability problems. The existence of these problems has served as a significant impediment to the widespread emergence of network-centric operations. For example, in the air-to-air mission area, combat ID remains a major challenge for Joint operations. Advanced air-to-air missiles can seldom be employed at maximum ranges because of the desire of war-fighters to positively identify detected aircraft and avoid fratricide.[7] Sufficient evidence exists to provide proof that focused investments in networking can significantly reduce the combat ID challenge and maximise the effective engagement range of air-to-air missiles as well as increase combat effectiveness, as described previously in the JTIDS vignette. As a result, defence planners have the option of increasing combat power by networking legacy systems and potentially forgoing large investments in "next generation" platforms.

[7] ibid, pp. 93–103

Invest Strategically

It may not be possible, because of resource constraints, for a nation to fully network its armed forces all at once. However, evidence from experimentation in the U.S Armed Forces indicates that focused, yet relatively small, investments in networking can have a disproportionate impact on the ability of a force to increase its combat power in high priority mission areas. The implication here is to invest initially in networking the force in the areas of the force that will have the highest payoff to operational commanders. In some cases, the operational payoff of network-centric operations can be so significant that it can reduce the size of a force required to prevail in a given operational situation.

CONCLUSION

The networking of a force involves extending the information domain and creating conditions for the emergence of network-centric operations. The source of the increased combat power associated with network-centric warfare is non-intuitive. However, emerging evidence points to important relationships between shared information, increased shared situational awareness and increased combat power. The evidence of the power of network-centric warfare collected to date highlights the importance of experimentation in developing and refining concepts and doctrine for network-centric operations, as well as the benefits that can accrue to a war-fighting force that masters the concepts of network-centric warfare.

5

From Network-centric to Effects-based Operations

Applying Information Age Warfare to Military Operations in Peace, Crisis and War

Dr. Edward A. Smith, Jr., Boeing WSA

(Excerpt from "Effects-based Operations: Applying Network-centric Warfare in Peace, Crisis and War", published by DOD CCRP, September 2002)

EXECUTIVE SUMMARY

The terrorist attacks of September 11, 2001, fundamentally changed our security environment. The system of strategic deterrence in place since the beginning of the Cold War visibly collapsed. In place of mutually assured retaliation came the threat of terrorists armed with weapons of mass effect whom we may not be able to identify and who have no homeland at risk. The existing "balance of terror" became, with 9/11, unbalanced. Now we are trying to fashion a new strategic deterrence that relies not so much on retaliation as on prevention: either stopping the terrorists outright, deterring the sponsors, or convincing them that terror cannot succeed. Where strategic nuclear deterrence was the *sine qua non* of the Cold War, this new prevention-based deterrence demands a balanced application of both civil and military power to shape behaviour. This shaping of behaviour is the essence of effects-based operations.

To help us deal with the pressing problems of the post-September 11 world, we have three on-going technological revolutions in sensors, information technology and weapons. We can use the technologies simply to achieve incremental improvements in force effectiveness. But to do only this would miss their real potential. These same technologies can

enable us to think differently about how we organise and fight. Indeed, this is what network-centric operations are about. But this too is not enough. Network-centric operations are a means to an end. Their true impact derives from how they are applied. Narrowly applied, they would produce more efficient attrition; yet they clearly can do much more. The concept of effects-based operations is the key to this broader role. It enables us to apply the power of the network-centric operations to the human dimension of war and to military operations across the spectrum of conflict from peace, to crisis, to war—just what a new strategic deterrence demands.

DEFINING EFFECTS-BASED OPERATIONS

The broad utility of effects-based operations grows from the fact that they are focused on actions and their links to behaviour, that is, on stimulus and response, rather than on targets and damage infliction. They are, hence, applicable not only to traditional warfare but also to military operations short of combat. Effects-based operations are not new. Good generals and statesmen have always focused on outcomes and, specifically, on the human dimension of war, for example, will and shock. Indeed, we can trace how the principles of effects-based operations have functioned in hundreds of crises and conflicts to distil a straightforward definition.

> "Effects-based operations are coordinated sets of actions directed at shaping the behaviour of friends, foes and neutrals in peace, crisis and war."[1]

[1] Effects-based operations are not defined in terms of a process because we logically cannot describe a procedure for planning and executing effects-based operations until we have first defined what those operations are.

The concept of effects-based operations, thus, focuses "coordinated sets of actions" on objectives defined in terms of human behaviour in multiple dimensions and on multiple levels and measures their success in terms of the behaviour produced. The "actions" include all facets of military and other national power that might shape observers'—"friends, foes and neutrals"—decisions. Military actions, for example, might include air strikes, but extend equally to a host of other military actions such as the role of manoeuvre apart from combat—a major aspect of almost all crisis operations. Actions, thus, encompass operations "in peace, crisis and war", not just combat.

If we look closely at real-world crisis and combat operations, some rules of thumb for effects-based operations quickly emerge. Actions create effects not just on the foe but also on anyone who can observe them. Effects can occur simultaneously on the tactical, operational, military strategic and national or geo-strategic levels of military operations, in domestic and international political arenas and in the economic arena as well—often with non-linear results. Effects cannot be isolated. All effects, at each level and in each arena, are interrelated and are cumulative over time. Finally, effects are both physical and psychological in nature.

OPERATIONS IN THE COGNITIVE DOMAIN

Effects-based operations can be described as operations in the cognitive domain because that is where human beings react to stimuli, come to an understanding of a situation and decide on a response. To create an effect, an action first must be "seen" by the observer who will then perceive it, interpret it, and "understand" it against a backdrop of his or her prior experience, mental models, culture and institutional ties, and translate this perception into a "sense" of the situation. Finally, this sense will be balanced against the options perceived to be available to produce a set of decisions and the reactions—if any—that constitute a response or "behaviour". This cycle of actions and reactions will be repeated many times at multiple levels during the course of a crisis, a war or even a peacetime interaction.

The cognitive cycle suggests three levels of complexity in effects-based operations.

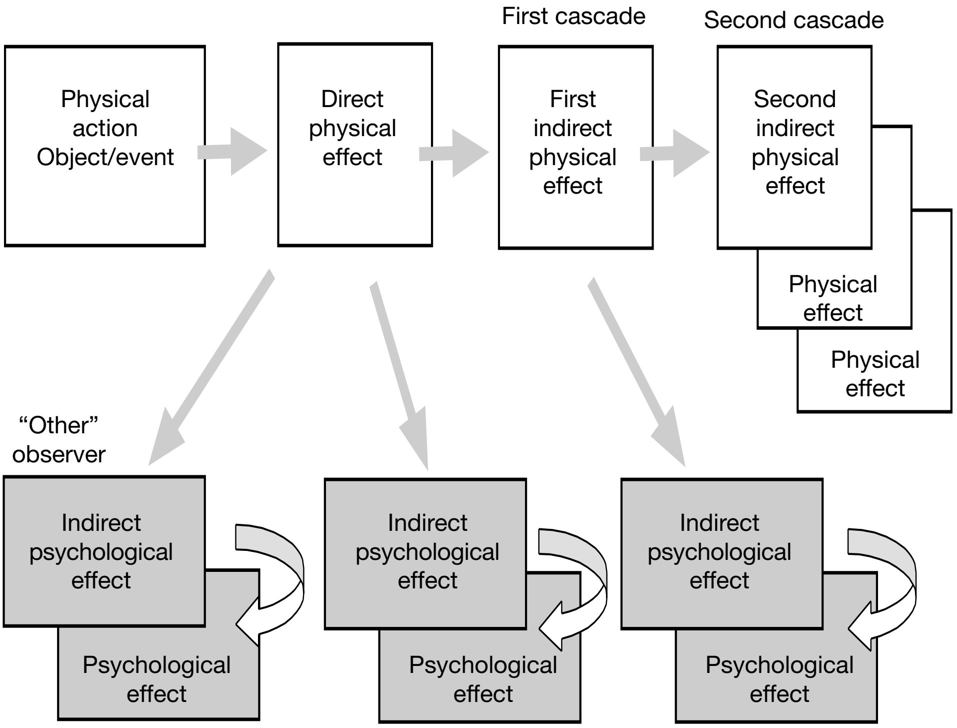
First, we must somehow orchestrate our "actions" to present a particular picture to the observer. However, the observer will "see" not only what we do but also how we do it, that is, the scale of our action, its geographic and operational scope, and its timing—speed, duration and synchronicity. But, he will "see" only those facets of the action that his data and information collection capabilities permit.

Second, we must be able to identify a link between a particular action or set of actions and the effect we seek to create. But, cognitive processes contain so many variables that we cannot reliably trace a cause-and-effect chain from a specific action to a specific reaction. We, therefore, need to think in terms of the kinds of potential physical and psychological effects: destruction, physical attrition, chaos, foreclosure, shock and psychological attrition. These categories are not mutually exclusive but are elements in an overall effect that will itself vary from one situation to the next, from one level to the next, from one observer to the next, and over time.

Third, since effects are interrelated, the direct effects we create will tend to cascade into successions of indirect physical and psychological effects in ways that are different and not entirely predictable. Physical effects will tend to cascade in the manner of falling dominoes while psychological effects will tend to cascade almost explosively limited only by the speed and scope of communications. Our operations may exploit these cascades to amplify the impact of our actions or may have to control them so as to check unwanted collateral effects.

To plan and execute effects-based operations, we need not know exactly how an observer will think or predict exact outcomes. Our object is to identify a series of the most likely outcomes that is sufficient for planning. For this, we need to know the nature of the stimulus we are creating and the decision-making problem it will present to observers—friend and foe alike. And, we need to know something of observers' decision-making processes so as to assess the influences upon the decisions, such as institutional biases, prevailing mental models, and so on. Given this knowledge, we can estimate how the various aspects of our actions might be perceived and what options might be considered in response.

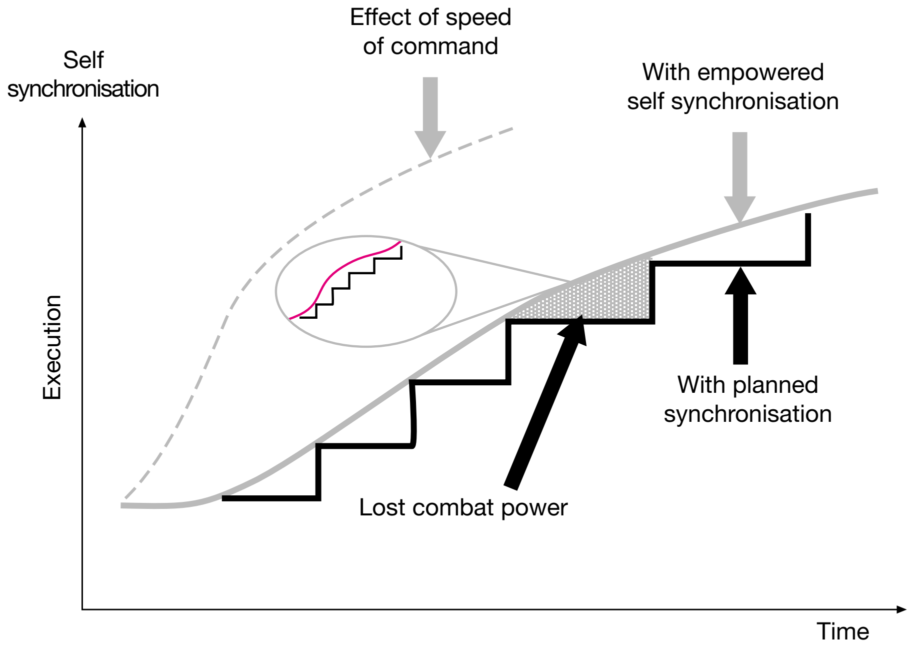
Managing Effects Cascades


First cascade
Second cascade
Physical action Object/event
Direct physical effect
First indirect physical effect
Second indirect physical effect
Physical effect
Physical effect
"Other" observer
Indirect psychological effect
Psychological effect
Indirect psychological effect
Psychological effect
Indirect psychological effect
Psychological effect

We must also be able to adapt agilely to changing situations. For this, we will require feedback: first, as to whether our actions had the direct effect intended and, second, as to any change in behaviour created. But, how do we get this feedback? Clearly, there are many parts of the cognitive process we will not be able to observe. Nonetheless, there are observables we can exploit. If an action involves destruction, damage assessment remains an index of whether the direct effect sought was achieved. Similarly, a system's physical performance can provide an index of direct effect. Likewise, assessment of an organisation's performance can provide an index of its reaction to the stimulus. Finally, we might take a cue from indications and warning intelligence and aggregate large numbers of small indicators any one of which might by itself be meaningless but which, when combined in the proper algorithm, can provide feedback on behaviour.

NETWORK CENTRIC OPERATIONS: OPTIONS, AGILITY, COORDINATION AND KNOWLEDGE MOBILISATION

Network-centric Operations



Source: New Sciences and Warfare, VADM A.K. Cebrowski, 21 August 1998

Despite its complexity, the above is not an impossible task. We have been dealing with these challenges on an ad hoc basis throughout history. The good news is that we now can tap the technologies and think of network-centric operations to provide four key ingredients of successful effects-based operations: options, agility, coordination and knowledge mobilisation.

Options

The ability to link diverse and geographically separated capabilities offers decision-makers a wide range of options to tailor our actions precisely to a situation and set of observers so as to increase their impact. In a sense, networking permits the probability of kill, Pk, of attrition-based metrics to be replaced by a "Po" effects-based metric in which the "o" is the probability of a given capability producing a useful option to deal with a given situation.

Agility

The responsiveness of networked forces with shared awareness and speed of command provides the agility to adapt to an intelligent adversary's actions by enabling us to shape and re-shape our options and actions amid the give-and-take of battle and crisis operations.

Coordination

Shared situation awareness and understanding of command intent, coupled with the capacity for synchronisation and self-synchronisation, enable us to coordinate complex effects that will span four levels of military operations and military political, diplomatic and economic arenas so as to produce a unity of effect in which diverse actions build on each other synergistically.

Knowledge Mobilisation

Finally, and most importantly, success in effects-based operations will hinge on how well we mobilise knowledge and expertise—from across the nation or across a coalition—to provide timely relevant support to decision-makers at all levels. Flexible, responsive networking can bring this breadth of knowledge to bear.

In brief, network-centric operations are indeed a means to an end, and effects-based operations are that end.