

pointer

<http://www.mindef.gov.sg/safti/pointer/>

Vol. 33 No. 3 [2007]



Navies and Maritime Security –
A Republic of Singapore Navy Perspective
by RADM Chew Men Leong

Comprehensive Maritime Domain Awareness –
An Idea Whose Time Has Come?
by LTC Irvin Lim

Building Maritime Security in Southeast Asia –
Outsiders Not Welcome?
by MAJ Victor Huang

The Top 3 Prize-Winning Essays of
CDF Essay Competition 2006



Editorial Board

Advisor
Chairman
Members

BG Jimmy Tan
COL Chan Wing Kai
COL Joseph Leong
COL Tan Swee Bock
COL Ng Kok Wan
COL Harris Chan
COL Ng Kin Yi
COL Siow Chee Khiang
LTC Irvin Lim
LTC Manmohan Singh
MR Wong Chee Wai
MR Kuldip Singh
A/P Aaron Chia
MR Tem Thiam Hoe
SWO Francis Ng
MAJ Andy Ang
MR Sim Li Kwang
MAJ Psalm Lew
MAJ Lim Kheng Choon
MAJ Terence Quek

Editor
Assistant Editor
Adjunct Editors

POINTER is a quarterly publication of the Singapore Armed Forces. The opinions and views expressed in this journal do not necessarily reflect the official views of the Ministry of Defence.

The Editorial Board reserves the right to edit and publish selected articles according to its editorial requirements.

Please address all contributions and correspondence to:



Editor, *POINTER*
SAFTI MI, Military Studies Branch
500 Upper Jurong Road
Singapore 638364

or fax 6799-7758. You can also contact the Editor at
tel no. 6799-7752/7755.

Our website is <http://www.mindef.gov.sg/safti/pointer>
and our email contact is <pointer@starnet.gov.sg>

▲ On the cover: The background image on the cover is actually a watermark image of four flag bearers featured on *To Command*, a publication of SAFTI MI

Copyright ©2007 by the Government of the Republic of Singapore. All rights reserved. The articles in this journal are not to be reproduced in part or in whole without the consent of the Ministry of Defence.



CONTENTS

EDITORIAL

FEATURES

- 5 **Navies and Maritime Security – A Republic of Singapore Navy Perspective**
by RADM Chew Men Leong
- 13 **Comprehensive Maritime Domain Awareness – An Idea Whose Time Has Come?**
by LTC Irvin Lim
- 27 **Building Maritime Security in Southeast Asia – Outsiders Not Welcome?**
by MAJ Victor Huang
- 45 **Network Enabled Capability – Dream or Reality?**
by Commodore(Ret) Patrick Tyrrell
- 54 **Beyond the Velvet Curtain of Transformation – How the Future of Warfare will be Shaped**
by CPT Gareth Wong
- 66 **Diffusing the Fog of War – Superior Decision-Making in a Networked Environment**
by MAJ Liew Hin Ban

CONTENTS...cont'd

- 81 **Developing the Thinking Competency of SAF Leaders**
by LTC Lim Choon Peng

TECH EDGE

- 93 **Software Defined Radio Design for an IEEE 802.11a Transceiver using Open Source Software Communications Architecture (SCA) Implementation::Embedded (OSSIE)**
by MAJ Leong Wai Kiat, Chris

VIEWPOINT

- 106 **Beyond Deterrence and Defence**
by Mr Toh Boon Kwan

BOOK REVIEW

- 109 **Colonel John Boyd – The Man, His Contributions and Some Reflections for ‘Personnel’ Transformation**
by CPT Phua Chao Rong, Charles

FEATURED AUTHORS

- 114 **Robert Coram and Grant T. Hammond**

PERSONALITY PROFILE

- 118 **General Sudirman**

EDITORIAL

Global trade has increased substantially in the past few decades, facilitated in part by communication and technological advances. As the sea remains the most cost-effective way to transport increasing quantities of goods, we can expect maritime trade to continue growing in volume and significance. To illustrate, the Straits of Malacca and Singapore carry over 30% of the world's trade and 50% of global oil shipments, including 70% of Japan's oil imports and 80% of China's oil imports. These straits are the arteries that connect the economies of East Asia with those of Europe and the Middle East. Being a strategic choke point, any disruption to passage in the straits will have severe repercussions on the global supply chain.

Maritime trade is already affected by piracy and smuggling, and is a potential target for maritime terrorism. Security measures to tackle such dangerous and illegal activities and threats have been taken by many governments individually or multilaterally, while maritime experts and analysts have actively discussed such issues in public and academic forums.

In this issue, we are delighted to feature three articles on the important topic of maritime security. In the article "Navies and Maritime Security – A Republic of Singapore Navy Perspective", our Chief

of Navy, RADM Chew Men Leong, shares with us that the challenges of maintaining national security – of which maritime security ranks high in Singapore's priorities – has become more complex in recent years due to the changing strategic environment. As contemporary challenges to maritime security cut across national boundaries and are multifaceted, he posits that navies by themselves are not sufficient, and no single organisation or country by itself has the complete wherewithal to tackle the plethora of maritime threats. To deal with these threats effectively, RADM Chew elaborates on a new paradigm of national security that he believes is necessary – one that is founded on strong inter-agency cooperation and greater international collaboration.

In "Comprehensive Maritime Domain Awareness – An Idea Whose Time Has Come?", LTC Irvin Lim draws attention to the perils confronting sailors, as well as nations of today and tomorrow, that are transnational in nature and multi-modal in trajectory. To improve marine safety as well as maritime security, he argues that Comprehensive Maritime Domain Awareness (CMDA) is something that nations, who place a high premium on the unimpeded flow of global commerce, should work together to achieve. His essay elaborates on the benefits that CMDA presents, the developments thus

far, and the challenges ahead. Given the contiguous and porous nature of maritime boundaries, he contends that the creation of a robust, reliable and resilient CMDA network will launch a new era of unprecedented maritime safety and security cooperation that is in the interests of the wider international maritime community.

Arguing that effective maritime security cooperation in Southeast Asia can be achieved only under a neutral multinational framework is MAJ Victor Huang and his award-winning article “Building Maritime Security in Southeast Asia – Outsiders Not Welcome?”. After examining the littoral states that border the Malacca Straits, he evaluates their willingness to cooperate. He then surveys recent attempts at maritime cooperation, analyses the factors for success or failure, and discusses how extra-regional players can contribute toward meaningful maritime security cooperation. Highlighting the littoral states’ experience in maritime cooperation, he concludes that they appreciate the assistance of extra-regional stakeholders – but only within limits that are highly circumscribed and not politicised.

In “Network Enabled Capability – Dream or Reality?”, Commodore(Ret) Patrick Tyrrell shares with us his thoughts on the United Kingdom’s

Network Enabled Capability (NEC) and its role in effective command and control. He postulates that while technology has revolutionised many aspects of military doctrine, it cannot change the behaviour of the human element. The bottom line is that decision-making remains a command function, and the biggest deterrent to effective decision-making is data and information overload. He asserts that though technology can help, without the ability to take effective decisions, NEC is a wasted asset. Only when the right people and right technology are employed, with the right doctrine and training put in place, can the NEC dream become a reality.

In this issue, we are also pleased to publish the top three essays of CDF Essay Competition 2006. We believe these winning essays contain pertinent gems that may help to improve our operational concepts, doctrines and organisation. In publishing the winning entries, we hope to facilitate knowledge management and exchanges, and make *POINTER* a useful source of reference.

Finally, it gives us great pleasure to announce that CDF Essay Competition 2007 is now open. Do check our website for more details. We look forward to receiving your entries!

Editor, *POINTER*

Navies and Maritime Security – A Republic of Singapore Navy Perspective

by RADM Chew Men Leong



Introduction

The primary goals of Singapore's national security are to safeguard its territorial integrity and guarantee the safety and well-being of its citizens. This requires the close monitoring of all potential threats, maintaining credible defences to deter, and if and when necessary, to respond decisively should deterrence fail. These will remain as the basic building blocks of the national security strategy for Singapore and possibly other countries like it. However, the challenges of maintaining national security has become far more complex in recent years. Changes in our strategic

environment call for a continuous reassessment of what needs to be done and the setting of new priorities if we want to enhance our national security.

The Changing Strategic Environment

One critical element for this shift has been globalisation. The security and economic well-being of all our countries is increasingly tied to factors far beyond our borders. In the economic sector, modern production is based on integrated supply chains that spread across the world. Thomas Friedman gave a sharp illustration in his best-selling

book, “The World is Flat”¹. Friedman traced the global supply chain behind the manufacture of the ubiquitous Dell Inspiron notebook. He noted that the Intel processor came from an Intel factory either in the Philippines, Costa Rica, Malaysia or China. The memory chip came from either South Korea, Taiwan, Germany or Japan. The graphics card was shipped from companies located in China. The keyboard came from either Tianjin, Shenzhen or Suzhou in China. The LCD display was made in either South Korea, Japan or Taiwan. The wireless card came from either an American-owned factory in China or Malaysia, or a Taiwanese-owned factory in Taiwan or China. The battery came from American-owned companies in Malaysia or Japanese-owned companies in Mexico, Malaysia, China or South Korea. The hard disk drive came from American-owned or Japanese-owned factories in Singapore, Thailand or the Philippines. The power cord came from a British-owned company with factories in China, Malaysia and India. And the list goes on. This clearly illustrated how the inter-connectedness is fuelling a rapid growth of global supply chains for manufacturing. The same pattern is also seen in the critical energy sector. For the global economy, the disruption of these chains would have widespread systemic implications.

The bulk of the world’s manufactured goods, components, material and energy is transported by sea. Unfortunately, sea lanes straddle various zones of sovereignty, and are governed by overlapping national and international regimes. Regardless of whether ships are travelling in isolation at sea or next to one another at choke points, they are vulnerable.

Coming to the Southeast Asia region, the security of sea lanes takes on particular importance. The Malacca and Singapore Straits carry over one quarter of the world’s commerce and half the world’s oil. The range of potential threats in this part of the world, as with many other strategic waterways, is wide. It ranges from petty theft to more violent acts including piracy and sea-jacking, to possible terrorist attacks. Inspiration for terrorist attacks can be gleaned from incidents such as the attack on MV Limburg off the Yemeni Coast², the attack on Al-Basrah Oil Terminal in Iraq³ and the USS Cole incident⁴. One nightmarish scenario may involve a strategically directed attack of a chemical carrier, possibly paralysing or closing an entire port or harbour in the region.

A New Paradigm of National Security

It is therefore not surprising that keeping sea lanes safe and secured has taken on greater importance and has come into sharper focus. Maritime security is one critical issue that ranks high in Singapore’s national security priorities, as with many countries around the world. Contemporary challenges to maritime security cut across national boundaries. They are multifaceted in that they tend to cross sectoral boundaries between enforcement agencies, port authorities and shipping associations. No single organisation or country has the complete wherewithal to tackle the plethora of maritime threats by itself. Instead, a new paradigm of national security is necessary, one that is founded on strong inter-agency cooperation and greater international collaboration.

Navies play a crucial role in this. In fact, when it comes to international collaboration, navies in the world already have a head start. Navies have been cooperating and working well before the phenomenon of “globalisation” and “networking” became buzzwords. Navies can well appreciate one another’s concerns and readily share best practices. Likewise, the Republic of Singapore Navy (RSN) plays a vital role in collaborating with others in flashing out these new paradigms.

Inter-Agency Cooperation

A comprehensive maritime security solution starts with a shared dialogue at the national level. A dialogue amongst maritime agencies on where security risks may exist and how best to reduce these risks collaboratively is critical. Pooling the various domains of expertise, experiences and ideas overcome blind spots and unwitting gaps, and help lead to a systematic adoption of risk-reduction strategies. In Singapore, this dialogue takes place at the Maritime Security Committee (MSC). The MSC is an inter-ministry

and inter-agency set-up that comprises representatives from the Ministries of Defence, Foreign Affairs, Home Affairs and Transport, and the intelligence and defence technology agencies. It develops the strategy for maritime security, as well as identifies and implements the operational measures to reduce threat risks. It also helps to foster a tightly-knitted community of agencies concerned with maritime security.

Singapore’s maritime security strategy comprises a few key components, all centred on tight inter-agency cooperation as its primary building block.

The first component is situational awareness. One can only respond when a threat is known to exist. Amidst the 1,400 ships that traverse the Strait of Singapore daily, Singapore is building up capabilities to detect anomalies in order to cue decisive response effectively. The challenge, of course, is to collate seemingly insignificant data, translating them into a coherent situation picture, and then “filtering out” the anomalies. In Singapore, the networking of sensors ashore and



The USS Cole and MV Limburg incidents; contemporary challenges to maritime security cut across national boundaries and are multifaceted, no single organisation or country has the complete wherewithal to tackle them by itself.

afloat from all agencies helps to track and monitor all shipping in our waters. Overlaid is a plethora of traffic control schemes prescribed by the Maritime Port Authority (MPA) to channel the movement of vessels of concern to prescribed routes and anchorages. This enhances surveillance significantly. Any vessel that strays outside the designated routes and areas can be flagged out for attention immediately. Vessels carrying dangerous cargo such as liquefied natural gas and chemicals are of concern. So are small craft, including fast ferries, pleasure and trade craft, that can be rapidly converted into potential weapons. To better track small boats that are not covered by the Automatic Identification System (AIS) regime, Singapore has instituted a Harbour Craft Transponder System or HARTS, a tracking system installed on all Singapore-registered small craft below 300 tonnes. In our ports, gamma-ray scanners are employed to detect hidden compartments and other anomalies within selected shipping containers. Coupled with data-mining and anomaly detection capabilities, the odd patterns may just stand out early enough for agencies to mount a timely response.

Singapore has always subscribed to the belief that an ounce of deterrence is worth more than a pound of cure. Any defensive measure taken by the maritime security forces must be visible and send a strong deterrence message. A wide spectrum of visible obstacles can thwart potential attempts. Even a suicidal terrorist would be deterred if his chances of success are deemed to be too slim. Active and regular presence at sea, bolstered by regular demonstrations of counter-terrorist tactics, will show preparedness and

address any perceived vulnerabilities. Today, the RSN works hand-in-glove with the Police Coast Guard to share the responsibility of showing presence and maintaining protection within Singapore's waters. Patrol sectors are aligned to provide better coverage for vital installations and anchorages. Selective escorts of merchant ships by maritime security forces are conducted on a daily basis to improve security. The RSN has developed a sea marshal programme called Accompanying Sea Security Teams. These teams comprised highly trained personnel from the RSN and the Police Coast Guard, and are deployed on-board selected vessels within Singapore waters to deter and prevent possible terrorist acts. Checks on small craft and trade craft are also carried out prior to their port entry. Force protection measures at the naval bases are enhanced when visiting foreign warships are berthed in our bases. All these constitute collaborative measures by agencies to cast an effective deterrent presence in our waters. The end game is to deter and reduce risk of maritime terrorism. Yet in the process, these operational measures also collectively help to eliminate piracy, sea robberies and smuggling activities.

However, deterrence may not always work, hence the need for decisive response. The spectrum of threats to maritime security we face today demands for a range of flexible and calibrated response capabilities. These encompass robust self-defence measures, an array of non-lethal as well as lethal responses, and a range of board, search and seizure capabilities. These measures may be implemented proactively, reactively or as a consequence action. Interestingly,

warships are traditionally designed and built for rather specific roles – frigates, patrol vessels, support ships and so on. Given the wide spectrum of operations today, many of our ships have to undertake maritime security and other roles, which may not necessarily be what they were designed for originally. The detection and interdiction of small boat threats in force protection are becoming just as important as anti-missile defence suites. Sufficient modularity in ship design is prized to enable naval ships to carry and launch a variety of capability modules for a wide range of threat responses, ranging from unmanned vehicles to rigid hull inflatables to non-lethal weapons. The ability to launch and operate unmanned surface vehicles to patrol, survey or even intercept a suspicious boat potentially on a suicide mission becomes an important capability proposition. The ability to network and share information directly with maritime port authorities and police boats becomes as important as conventional datalink requirements for warfighting. As navies seek greater flexibility in mounting a range of responses and optimising modular capabilities, there is a need to leverage on the combined resources of partner agencies.

International Collaboration

Maritime security has to be a transnational and collaborative effort. Maritime threats have no regard for national boundaries. Their effects are felt on the littoral states, as well as on all trading nations around the world. Collaboration between countries based on international law and conventions is a must, if we wish to deal with these threats effectively.

Again, the starting point of any collaboration lies with dialogue. Multilateral dialogue, in particular, is an important process for defining and clarifying what we can pursue in the regional maritime security agenda. While countries may not always achieve full agreement on every issue, where we do agree can be significant. Where there is agreement, there is a basis to move forward in terms of collaboration. From shared perspectives, interests and agreements, we can move to the development of practical cooperation and capacity building to tackle the common maritime security threats.

In the region where Singapore is located, the progression from dialogue to understanding, and then to action, is already taking place. Maritime security has been discussed extensively over the past three years in a number of fora, including the ASEAN Regional Forum, the Western Pacific Naval Symposium, the Five Power Defence Arrangements, and most significantly, at the Shangri-La Dialogue. The frank discussions have helped the region and partner nations to progress from understanding to collaboration proposals.

In the Shangri-La Dialogues, consensus was achieved on the adoption of three principles for maritime security cooperation. First, the primary responsibility of maritime security in the Malacca Straits lies with the littoral states. Second, there is a role that the international community, agencies like the International Maritime Organization and major user states, can play. Third, measures taken must be in accordance with international law and respectful of the sovereignty of the littoral states.

With this consensus, the region was able to move quickly from principles to cooperative action. In July 2004, Indonesia, Malaysia and Singapore bolstered existing bilateral arrangements with the launch of the trilateral Malacca Straits Sea Patrols. The patrols provide a 24/7 naval presence in the Malacca and Singapore Straits and enhance coordination among the respective navies' ground units and operations centres. This was followed in September 2005 by the "Eyes in the Sky" maritime air patrols, an innovative idea for multinational air patrols that was raised by Malaysian Deputy Prime Minister and Defence Minister, Dato Sri Najib Tun Razak. The "Eyes in the Sky" patrols have an innovative design which ensures that the littoral states are in the driver's seat while opening up opportunities for the participation of non-littoral states in the future. These two initiatives have shown good results as the incidences of piracy in the Malacca Straits have dropped since their inception. The Joint War Committee (JWC) of London-based Lloyd's Market Association also announced the removal of Malacca Straits from its list of war-risk areas⁵ in August 2006.

The security of the Malacca and Singapore Straits is a complex issue that can only be tackled with the cooperation of regional players and those beyond. By sharing and optimising respective capabilities and assets, the two initiatives, now collectively known as the Malacca Straits Patrols, laid a good foundation from which we can do more – to further improve our interoperability in shared situational awareness, deterrence

against threats to maritime security and responsiveness to incidents at sea.

A useful way to build greater capacity for collaboration and nurture a foundation of trust and understanding, is to extend the breadth and depth of the multilateral exercises amongst regional and extra-regional navies. The progress in this area in recent years has been encouraging. Three years ago, the Ministers of the Five Power Defence Arrangements (FPDA) agreed to expand FPDA activities to address non-conventional threats. Since then, maritime security serials have been incorporated in FPDA exercises, including the recently concluded major exercise *Bersama Padu*. The Western Pacific Naval Symposium or WPNS for short, a forum that brings together 24 Asia-Pacific Navies has also made considerable progress in developing maritime security cooperation. In 2005, 19 WPNS navies and 15 ships took part in an inaugural sea exercise to build capacity for collaboration. In 2007, the RSN successfully hosted the second WPNS Multilateral Sea Exercise with 18 ships participating. To date, two WPNS Maritime Security Information Exchange Seminars have been held in Singapore. In the most recent seminar, a frank exchange of hitherto operational information by one of the regional navies had helped to build a better understanding of the maritime situation in the Malacca Straits. These multilateral activities help enhance interoperability and create a foundation of trust upon which future collaborative initiatives can be built.



Participants of the WPNS Multilateral Sea Exercise; multilateral activities help enhance interoperability and create a foundation of trust upon which future collaborative initiatives can be built.

Maritime information sharing is yet another useful way to improve maritime security. Following the 17th International Seapower Symposium in 2005 and other regional fora, there seemed to be converging interests and growing recognition that information and knowledge sharing amongst navies is critical in combating transnational crime and maritime terrorism. As no navy can achieve 100% comprehensive awareness alone, information sharing amongst the various users of the sea is necessary. The Regional Seapower Symposium's Virtual Regional Maritime Traffic Centre initiative led by the Italian Navy, and the US Navy's initiative of establishing the Cooperative Maritime Forces Pacific, a maritime information sharing network based on the CENTRIX system⁶, both point to this global inclination towards information sharing. They also highlight the importance of collaboration in exchanging and integrating information to build a comprehensive maritime picture.

In the same light, the RSN sees that the time is right to help bring collaborative information sharing efforts up one notch within this region. To better support maritime information sharing, the RSN recently put forth the development and use of the Regional Maritime Information Exchange (ReMIX). ReMIX is an Internet-based platform that will serve as a readily accessible web portal for the sharing of operational information amongst WPNS navies. For example, ReMIX can facilitate timely sharing of information pertaining to piracy incidents, missing or hijacked vessels, vessels in distress, maritime accidents and other incidents of concern. Separately, another information sharing system has been introduced by the RSN for trial use by the littoral states under the ambit of the Malacca Straits Patrol initiative. Collectively, these initiatives will enhance the overall situational awareness and facilitate better operational coordination against threats to maritime security.

Conclusion

The security and well-being of our countries are linked together more intimately than we could have imagined only a decade ago. The confluence of greater dependency on sea lanes for trade flow and the rise in a plethora of non-conventional and terrorist threats pose new contemporary challenges to navies worldwide. The need for response by navies to these challenges has altered their priorities and capability sets. Yet, navies by themselves are not sufficient. The key to dealing with threats to maritime security lies in strong inter-agency cooperation and

enhanced international collaboration. A close working relationship amongst the various inter-government agencies is required to implement a comprehensive and robust risk reduction strategy, while collaboration on a multilateral basis amongst countries and their navies is critical in overcoming the wide-ranging and transnational threats to maritime security. Singapore will continue to work with the littoral states and like-minded countries to strengthen maritime security in the region in the years ahead. 

Endnotes

- ¹ Thomas Friedman, *The World is Flat – A Brief History of The Globalized World in the 21st Century* (New York: Penguin Group 2005), pp416-417.
- ² A small boat rammed into the MV Limburg, a 157,000 tonne crude-oil tanker, in a suicide boat attack off the coast of Yemen on 6 Oct 06. The hull of the tanker was damaged and one crewman was killed in the attack.
- ³ An attempted suicide attack against the Al-Basrah Oil Terminal, located about 19 miles from Iraq’s main port of Basrah, was staged by insurgents using an explosive-laden fishing boat on 24 Apr 04. Two US Navy sailors and one Coast Guardsman were killed in the attack but damage to the oil terminal was limited due to Coalition’s security efforts.
- ⁴ Al-Qaeda successfully staged a suicide bombing attack against the US Navy guided missile destroyer USS Cole on 12 Oct 00, while it was harboured in the port of Aden, Yemen. USS Cole was severely damaged and 17 sailors were killed as a result of the attack.
- ⁵ The Joint War Committee of the Lloyd’s Market Association added the Malacca Straits to its list of war-risk areas in June 2005 on the premise of an observed deterioration of the security situation in the strait. The Lloyd’s Market Association is an insurance body that advises the members of the Lloyd’s of London.
- ⁶ The Combined Enterprise Regional Information Exchange (CENTRIX) is a US-sponsored network system to facilitate coalition interoperability in support of military operations.



RADM Chew Men Leong assumed his current appointment as Chief of Navy on 31 Aug 07. A Naval Officer by training, he has held amongst others, the appointments of Chief of Staff (Naval Staff), Fleet Commander, and Head of Joint Plans and Transformation Department. RADM Chew is a SAF Overseas Scholar and SAF Postgraduate Scholar. He holds a Bachelor of Engineering (First Class Honours) in Electrical and Electronics Engineering from the Imperial College of Science, Technology and Medicine, U.K., as well as a Master of Science in Management from Stanford University, USA. A graduate of the Singapore Command and Staff Course in 1996, RADM Chew was the top Navy student of his class.

Comprehensive Maritime Domain Awareness – An Idea Whose Time Has Come?

by LTC Irvin Lim



“There is only a perspective seeing, only a perspective ‘knowing’; and the more affects we are allowed to speak about one thing, the more eyes, different eyes, we can use to observe one thing, the more complete will our ‘concept’ of this thing be.”

- Nietzsche¹

Introduction

In the Age of Exploration and Empires, where sailing into the unknown meant confronting certain peril, Henry the Navigator established a maritime centre in Lisbon to equip sailors with nautical knowledge, instruments and vessels to overcome the elements as they voyaged into new frontiers to discover new geographies of knowledge. Some 600 years later, with much of the seas well-charted and lands discovered, the idea of equipping sailors *and* maritime

agencies with (fore)knowledge to overcome perils *at* and *from* the sea is no less germane. The perils confronting sailors as well as nations of today and tomorrow, are transnational in nature and multi-modal in trajectory. And they carry with them potentially grave (inter)national maritime safety and maritime security implications.

Such maritime threats range from piracy, hijacking, the illicit trafficking of contraband and people as well

as terrorism and the proliferation of weapons of mass destruction that find carriage and conveyance through the world's increasingly congested waterways. In particular, the terrorist threat in the maritime domain remains a clear and present danger. To be sure, efforts to localise such maritime threats and their trajectories in the vast expanse of the world's waterways can be daunting, and may invariably end up no more and no less like searching for the proverbial needle in a haystack. Nevertheless, there is operational utility for knowledge built around vessel traffic tracking information that enhances awareness in real-time for priming responsive action against maritime threats. What is also equally clear is that no nation can go at it alone in such an expansive effort. There is therefore scope to build up relevant information-sharing expertise and capacity in order to facilitate more responsive collaboration between national agencies and the world's maritime centres to provide real-time visibility of the global flows of maritime traffic across the world's oceans.

The Need for Maritime Domain Awareness

Given the contiguous and porous nature of maritime boundaries, it is important for effective surveillance of the world's waterways. Even if achieving 'sea control' of the global commons in a *Mahanian* sense is but a *will-o-wisp*, the capability to 'see and sense' what moves on water at any point in time is something that maritime nations can work together to achieve in order to improve marine safety as well as maritime security

to safeguard their interests. It is now technologically possible to do so, even if technical hurdles remain. The key political challenge will be in securing the cooperation of countries to enmesh themselves in a web of maritime security information-sharing cooperation as a public good. Such information-centric cooperation will not merely be concerned with vessel traffic movement *per se*, but will also need to drill down, with some measure of confidence, into important vessel-centric risk profiling specifics like ownership, charterer, vessel cargo, crew manifests and even watercraft blueprints. Take the recent example of security concerns over almost 1,500 tonnes of explosives-grade ammonium nitrate used in mining operations that was shipped in and out of Botany Bay on five vessels that were registered in overseas ports such as Liberia and Antigua and Barbuda during the Sydney APEC summit in mid-September 2007. The vessels had crews from Myanmar, the Philippines and Eastern Europe who had reportedly not undergone background security checks.² While ammonium nitrate usage on the mainland is heavily regulated, it is apparent that vessels carrying such cargo along coastal waterways are not. The shipments highlight the risks involved, calling into question potential blind spots and differing enforcement standards of regulatory regimes associated with foreign shipping entering a nation's waterways. Making shipping secure remains a big challenge for the international community, as much of the heavy-lifting of the globalised trading economy is performed by ships that fly under 'flags of convenience', registered in tax havens with few minimum working

conditions and differing standards of security clearance for crews. Achieving Maritime Domain Awareness (MDA) will therefore require info-sharing, info-fusion and sense-making in order to cue responsive intelligence and operational coordination, as directed by decision-makers backed by relevant maritime legislation and shaped by strategy-driven policies.

The quest for the holy grail of domain awareness at sea is already well underway. In an ambitious attempt to better secure the overexposed maritime domain, the United States has embarked upon a comprehensive national effort to enhance homeland security by preventing hostile or illegal acts within the maritime domain. *The US National Plan to achieve Maritime Domain Awareness* has been drawn up in October 2005 as one of eight supporting plans in operationalising the *National Strategy for Maritime Security* (NSMS).³

Connecting Virtual ‘Strategic Hubs’: Vital Turn-Key to CMDA Success

Beyond homeland security re-orientation and re-organisation post-9/11, a key aspect of many of the above ground-breaking initiatives spearheaded by countries like the US, is the international dimension; the importance of recognising and leveraging on multilateral cooperation that is inclusive remains the turn-key for success. Enhancing maritime security is not wholly a domestic concern of one state’s national interest or responsibility, and states can ill afford to be provincial or parochial in tackling common maritime challenges that respect no borders. After all, many countries that depend on maritime trade for their survival also have active stakes in the safety and security of the seas and need to take *ownership in partnership*. In other words, they can play a critical role

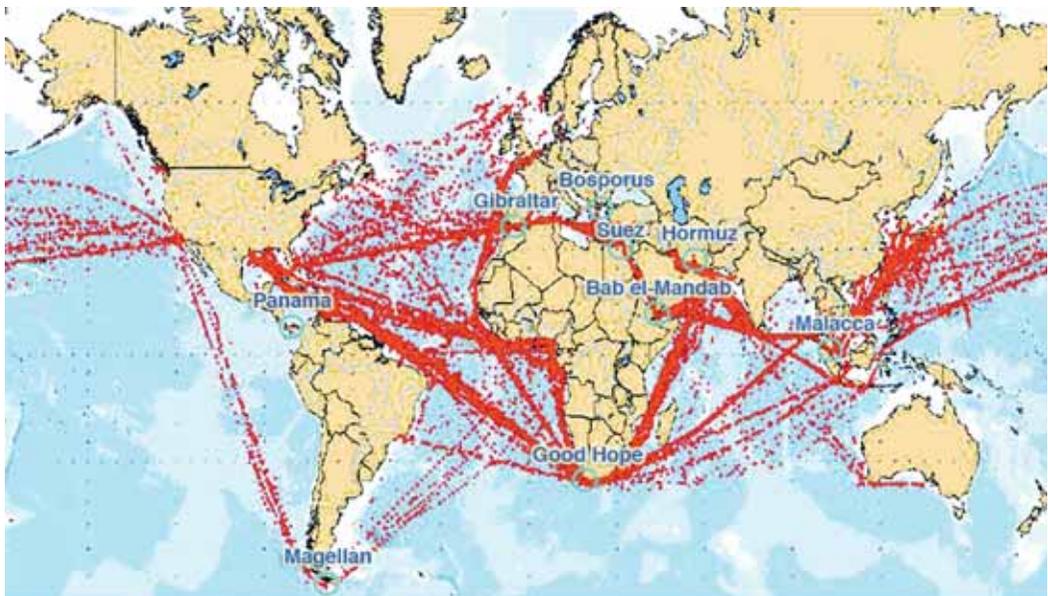


Diagram 1. Global Maritime Traffic Patterns and Strategic Choke Points.

in the overall effort to enhance maritime domain awareness by contributing their individual pieces of information within their respective maritime areas to complete the overall domain awareness puzzle.

When one looks at the global maritime traffic patterns, it is clear that the key maritime centres located at strategic choke points of maritime trade can serve as regional maritime information-sharing hubs for realising MDA; or in other words, introducing the ever-critical 'C' for 'Comprehensiveness' in the quest for a more watertight (inter)national MDA architecture.

This can be done by adopting an incremental willing-partner 'building-block' approach, with maritime hubs forging bilateral and multilateral intra-regional information-sharing networks, even as they seek to link-up with maritime regions beyond the region. All the while, the focus should be on making implementable steps that bridge targeted information gaps through information-sharing rather than idealistic leaps that attempt to cover scatter-shot all information gaps and ultimately achieve little in addressing real maritime security threats.

From Share-Hubbing to Sense-Making

In the short intervening years post-9/11, shipborne Automatic Identification System (AIS) is already widely used at sea. Together with Long Range Identification and Tracking System (LRIT) coming on-line, they form a simple yet powerful suite of ready-

made maritime tools that can be used in conjunction with other maritime information systems and sensors (ashore and at sea) which are being developed to enhance maritime situation awareness and traffic management. And more importantly from the maritime security perspective, they can aid in the early identification and tracking of 'Critical Contacts-of-Interest' (CCOIs) for possible maritime interdiction involving VBSS⁴ operations.

Given that the technology to do such 'virtual' border-less tracking via extraterrestrial means (satellite) is already on the cards, potentially side-stepping sovereignty/territorial concerns, the next bound or growth area for international maritime security information-sharing collaboration may well be in the joint development and sharing of expertise in fusing all the information together in order to better sense-make the information deluge downloaded from the various systems. Comprehensiveness should lead to greater comprehension. For example, innovations in *Risk Assessment Horizon Scanning* (RAHS)⁵ engines to pick up weak signals on mutating maritime threats at the macro-scenario level, can complement the development of advanced algorithms for delivering timely actionable threat evaluation at the operational contingency level.

The convergence of technological developments with heightened interest in operationalising global maritime information-sharing represents an opportunity for achieving *Comprehensive Maritime Domain Awareness* (CMDA). One signaling convergence effort is

already being made in Southeast Asia by Singapore to be a proactive partner-of-choice in enhancing maritime security. Seating astride strategic crossroads, with more than 50,000 vessels plying through the vital SLOCs of Southeast Asian waters annually carrying some one third of the world's trade and half of the world's energy supplies, Singapore is a "consequential place"⁶ in the global maritime supply chain. The island state recently announced the building of its Changi C2 Centre⁷ in late March 2007. This ambitious new facility, the first of its kind in the region, aims to serve as a regional maritime security hub when it is operational in 2009. It will provide a useful platform for nations to cooperate and respond more flexibly and effectively to a dynamic maritime security environment. Looking further ahead, it has the potential to develop into a strategic hub for a global CMDA network.

The Changi C2 Centre, a facility for multinational cooperation, built next to Changi Naval Base, is set to house three functional centres, namely, the Singapore Maritime Security Centre (SMSC), the Information Fusion Centre (IFC) and the Multinational Operations and Exercises Centre (MOEC). Envisioned to be the one-stop maritime information and response coordination centre, it will advance multi-agency cooperation and interoperability amongst national maritime agencies, and enhance Singapore's maritime security capabilities. The Changi C2 Centre will also enable international cooperation and interoperability between countries to promote maritime security in the region.

A Domain Under Construction – Multiple Points for Multiple Fixes

The importance of networking coalition partners for any sustainable, credible and deterrent maritime security effort has been well-recognised in other maritime security cooperation related ventures as well. Take US Chief of Naval Operations Admiral Mullen's eyebrow raising concept of the '1,000-Ship Navy' or what has now been termed the *Global Maritime Partnership Initiative* (GMPI) by the United States Navy (USN) as another telling example. The GMPI aims to make international maritime cooperation an important pillar of its new maritime strategy by building 'a global maritime network to provide maritime security'.⁸ The call for a global network is an acknowledgment of the utility in better networking the community of navies around the world to enhance information-sharing and promote interoperability at sea. Implicit in the USN's 'Thousand Ship Navy' (or GMPI) concept is the promising, if not polemical, metaphor of networking the power of a 'Thousand Ships' from diverse partnering navies around the world – polling together of resources and expertise, sharing of information for collaborative sense-making and coordinating responses against common maritime threats.

Granted that GMPI is still at a conceptual stage, identifying funding, technologies, personnel, organisation, and modalities for ensuring better coalition interoperability – at the sensitive but unclassified level – have yet to be ironed out. Nevertheless,

the impetus for developing a C4ISR capability to realise comprehensive maritime domain awareness is clear.

To be sure, such networks already appear to be under construction – as US Admiral Keating had alluded to when he said that the USN is keen to exchange information and share databases with the Indian Navy to make international maritime security more robust.⁹ Such fledgling bilateral proposals, should they translate into concrete initiatives over time by overcoming the various political and technical huddles, have the potential to kick-start and proliferate denser multilateral networks of maritime security information-sharing further downstream. In sum, multiple reference points provide for more accurate fixing, more reliable sense-making and more avenues for responsive action. For information-sharing to take place, the US military has developed its *Combined Enterprise Regional Information Exchange* (CENTRIX) system as one interoperable channel that can be used for promoting its global maritime network; one that the USN has routinely used while operating with coalition forces at sea. It also has the more capable and secure *Secret Internet Protocol Router Network* (SIPRNet) for dedicated operational use when needed.¹⁰ At the regional level, countries like Singapore have also developed their own unique *ACCESS* system for info-sharing to enhance interoperability at sea, as well as the Internet-based *Regional Maritime Information Exchange* (ReMIX) portal under the *Western Pacific Naval Symposium* (WPNS) framework to promote wider information-sharing among the navies of member countries.

Take the Malacca Straits again, as an example of how CMDA development can potentially take shape. In contrast to an earlier controversial US proposal to enhance maritime security by deploying forces in the Malacca Straits via the ‘*Regional Maritime Security Initiative*’¹¹ – which subsequently turned out to be a catalyst of sorts in precipitating greater littoral state cooperation – the building up of a global maritime security network to achieve CMDA, that includes the Malacca and Singapore Straits, should be more politically acceptable and operationally realisable. Furthermore, with the anticipation that security along the Strait of Malacca would be strengthened when ten new coastal surveillance radars, with sponsorship assistance by the US, are installed along the eastern coast of Indonesia’s Sumatra island in a couple of years¹², there may yet be new prospects for the sharing of situational picture in the Malacca Straits that can even be integrated into an expanded regional and global comprehensive maritime domain awareness network. Malaysia and Singapore have been running a comprehensive *Vessel Traffic Information System* (VTIS) for the Malacca and Singapore Straits for more than a decade now, and any augmentation with Indonesia’s entry into the extant arrangement from its side of the straits will no doubt further bolster maritime situation awareness, safety and security along the strategic waterways. Already, through their close cooperation in the *Malacca Straits Coordinated Patrols* and *Eyes in the Sky* at sea and from the air respectively, Indonesia, Malaysia and Singapore have

shown that building a culture of maritime security cooperation between states can provide concrete operational results and political dividends in enhancing the maritime security along the Malacca and Singapore Straits.¹³ Separately, Singapore and Indonesia have been successfully collaborating on *Project SURPIC* since 2005 to share the maritime situation picture to enhance surveillance and security of their common maritime borders along the Singapore Strait. Such multilateral and bilateral ventures, demonstrate that given sufficient political will, resource commitment and a balance of benefits for all involved, more can be done to shape and realise a more robust regional as well as global maritime security information sharing regime in the longer run. The new Singapore Changi C2 Centre that is being built is poised to be a key enabling node or hub in such a global CMDA network under construction.

Kick-Start by Plugging into Extant Maritime Centres

There is scope for a comprehensively equipped maritime centre such as Singapore's Changi C2 Centre to link-up and work with other (sub)regional maritime enforcement/information centres. For example, the US National Maritime Intelligence Center (NMIC) headquartered in Maryland, is an operational outfit manned 24/7 by Office of Naval Intelligence (ONI) and US Coast Guard personnel that enables the ONI to maintain a worldwide situational awareness on more than 18,000 ships underway on any given day.¹⁴ Another facility is NATO's Allied Forces Maritime Component Command

HQ Naples (CC-MAR Naples) that runs a Maritime Operations Centre. This Maritime Operations Centre, located close to the NATO Maritime Intelligence Coordination Centre, exchanges information with the national agencies of several NATO countries and works directly with NATO (*Operation Active Endeavour*) naval forces operating in the Mediterranean. It also exploits the synergies of sharing information with the experimental Joint Information and Analysis Centre (JIAC) which is structured as a fusion centre "to collect all available information and effectively collate, analyse and then disseminate data as actionable intelligence to the appropriate command".¹⁵ In so doing, JIAC acts as an honest broker for fused information that protects the supplying nation's sources even as it passes, in a timely manner, its sense-made output to nations and agencies that are most likely to be able to exploit it.¹⁶ Beyond establishing links with maritime security enforcement agencies, networking with other civil maritime safety and security set-ups should also be leveraged upon. One such other important centre that was recently launched in late 2006, also based in Singapore, is the *Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia* (ReCAAP¹⁷) Information Sharing Centre (ISC). The ISC collates and analyses information from ReCAAP member countries' *Focal Points*¹⁸, affected vessels/companies, other organisations or governmental agencies via its Information Network System to enable the timely dissemination and exchange of maritime safety and security information.



The NMIC and its watch floor in Maryland, USA; manned 24/7, it enables the ONI to maintain a worldwide situational awareness on more than 18,000 ships on any given day.

Although the ReCAAP ISC and Singapore's C2 Centre's IFC have different mandates and modalities of cooperation with their respective networks, their overarching mission to enhance maritime domain awareness through information sharing do not essentially differ. Given the mutually-reinforcing roles, there is scope for maritime security information-sharing agencies like the ReCAAP ISC to link-up to share information with Singapore's future Changi C2 Centre's IFC, in an integrated CMDA architecture even. Granted that it is still early days yet, and the fledgling ReCAAP ISC still has some way to go in building-up its research and real-time information-sharing capability via a distributed network of demonstrated operational utility. Nevertheless, should such promising developments live up to their potential, cooperative integration could kick-start the process for other maritime centres to be plugged into the information sharing network, and through its positive demonstration and exponential effect, cascade the growth of new offshoots linking-up other regional networks which contribute to the omnibus data-density of the envisaged CMDA project.

Grappling with Kinks in Information-Sharing

One paradoxical aspect of information sharing is dealing with the 'tension' of information security at the other end. Information sharing may reveal sensitive sources and compromise surveillance capabilities that some partners/parties may need to safeguard or selectively make privy as a matter of organisational/national interest. Therefore, information-sharing has to be secure while partnerships are being secured, to allay any unease over misuse and abuse of maritime security information. Related to these are governance and proprietary issues like whether there is a need for an 'honest broker', or who gets to be the 'system administrator' with 'policing rights' for such a 'detective' network, will need to be assuaged and addressed. What is clear is that the enabling technologies and evolving habits of cooperation need to be predicated on a relationship of trust with mutually-binding agreements for partnerships in any shared venture to work. In the end, finding practical ways of enhancing bilateral and multilateral information-sharing cooperation could well mean

defining mutually acceptable ‘rules of the game’ for information-sharing. These include data access-exchange policy, data integrity, source protection, and collaborative tools that are capable of forming ad-hoc sharing through datalinks between shore monitoring elements and surveillance assets at sea, as needed. In this regard, forging consensus over the governing parameters for release of information with potential partners will be a vital first step, before embarking upon any concerted effort at national and international levels to promote tangible maritime security info-exchange between willing and able partners from around the world.

Another hurdle relates to resistance against the introduction of additional layers of security information requirements with pervasive tracking that are seen as little more than new-fangled security tools that could potentially complicate the lives of seafarers by adding transactional friction and cost to shipping operations. Such fears and perceptions, founded or unfounded, have real effects on the level of industry support. Given the slew of additional security measures that have been introduced in recent years¹⁹, a certain wariness by the world’s commercial shipping community is to be expected and will need to be assuaged. This is especially the case when significant commercial sensitivity *and* industry competition surrounds the availability of proprietary information regarding importers and exporters, the nature of cargo and location of particular vessels. Over and above such market concerns, regulatory maritime regimes like UNCLOS and other related international conventions

and customary international law will also need to be appropriately reckoned with. This will be pivotal when framing the legal bases for securing buy-in on a viable CMDA project that critically needs to leverage upon industry participation and cross-boundary inter-agency collaboration.

In addition to managing such tensions, dealing with technical realities like connectivity issues between the various disparate systems, sense-making algorithms and system bugs will all require highly trained personnel with deeply-specialised knowledge to manage. In addition, how would the taxonomy of such a CMDA network look like and would it meet the needs of its users? The iterative adoption of an *Engagement, Experimentation and Evolutionary Capability Development* approach could be useful in preventing ‘white elephants’ and avoiding the creation of a ‘museum of experiments’, after all the collaborative effort and resource investments in realising a common recognised sea situation picture. Nevertheless, in the emergent ‘competition’ for the best practices and systems being developed to achieve a CMDA capability, some technical dead ends may well be necessary and only to be expected, with better innovative and cost-effective solutions overtaking and breaking new ground. Also, individual nodes in the CMDA network may well have specific requirements/limitations which lead to the incorporation of indigenous designs/processes that leverage on commercial off-the-shelf technologies *and* services as well. Already, commercially available options appear to have stolen the march on developing a rudimentary semblance

of what an envisaged CMDA network could potentially look like. Vessel Monitoring Systems (VMS) established by regional fisheries management organisations, such as the South Pacific Forum Fisheries Agency (FFA) and the Commission for the Conservation and Management of Highly Migratory Fish Stocks in the Western and Central Pacific Ocean (WCPFC), are making use of satellite Global Position System (GPS) technology to automatically plot the movement of participating countries' fishing fleets.²⁰ In another more vivid global example, *AISLive*, which is available *via subscription on-line*, was established just barely a few years ago in 2004, and now reportedly “covers over 1,200 places worldwide” with “more than 13,000 vessels under coverage at any one time”. It does this by linking AIS information nodes around the world into a virtual maritime map. As an attractive commercial proposition, its “state-of-the-art viewing software” allows shipping companies an easy means to track their fleets via what

has been touted as “the most cost-effective method of tracking vessels in real time today”.²¹ This Internet-based facility represents an avenue for real-time tracking information on ‘white-shipping’ that could be further harnessed. In terms of ready access to merchant shipping information, it should also be a path of least resistance insofar as CMDA is concerned.

In time, *network trust* and *technical-taxonomy challenges* associated with achieving CMDA should be surmountable. Whether a ‘standard fit’ system-of-systems approach is eventually adopted or not, for now at least, it appears that letting ‘a hundred flowers bloom’ approach is the default and most practicable option, with international organisations (governmental and non-governmental) in partnership with industry shaping system requirements and driving systems development. At some point downstream, when the various maritime information systems being developed



The AISLive represents an avenue for real-time tracking information on “white-shipping” that could be further harnessed. In terms of ready access to merchant shipping information, it should also be a path of least resistance insofar as CMDA is concerned.

around the world kick on-line, the higher leverage *knowledge challenge* will be in aggregating and distilling the information deluge, by situating potential maritime threats 'in context'. In other words, once the networks are in place, the real challenge or 'delta' to be achieved after all the data-gathering is sense-making. Sense-making is *the* value proposition of CMDA. Rather than 'seeing threats everywhere' and sounding-off with frequent false alarm rates that result in wasted efforts chasing down so many rabbit holes, as it were, a CMDA sense-making system will need to be programmed with advanced and adaptive user-requirement algorithms that help to separate 'the wheat from the chaff' in profiling, red-flagging and targeting CCOIs for timely alerts and appropriate action.²² The development of threat evaluation matrices, anomaly detection and critical-path analysis capabilities will be critical to sense-making. Effective innovation in a collaborative sense-making enterprise to achieve CMDA will require close cooperation and fostering a culture of trust and habit of cooperation; not an easy feat, especially if it is to be done virtually, taking into account differing perceptions of values, interests and sensitivity thresholds that can crop up to cloud the best of cooperative ventures, compounded by bureaucratic red-tape across real-world national boundaries. Capacity building and burden-sharing issues related to developing and maintaining maritime information-sharing infrastructure can also pose additional political hurdles that should not be underestimated as they can potentially hamstring information-sharing and related sense-making efforts. In parallel with technical sense-

making system development, training support and personnel development for the 'sense-makers' will also need to be given due attention for analysts to develop deep subject matter expertise in order to better customise requirements and exploit the range of tools provided by the various CMDA network systems to bridge information-gaps and siphon-out credible threats. Towards that end, the fostering of a Community of Practice (CoP) in a sense-making network built around maritime information-sharing hubs makes good sense. Such a maritime sense-making CoP will do well to 'reify' a new knowledge ecology of open information-sharing which supplants knowledge economy notions of transactional information exchange, and in so doing, replace exclusionary notions of need-to-know with an inclusive spirit of responsibility-to-share.

Going forward, even further downstream, assuming that some semblance of CMDA is eventually achieved, the CMDA project could well find new policy and operational need to take on cross-domain and multi-modal challenges of tracking not just vessels at port or under way at sea. After all, the maritime domain is not just about what moves on the surface of the water, but also in the airspace above, and arguably what is about to be put to sea via land. In this regard, close interface or access to civil air domain awareness (air-space management) information may well be necessary. That said, taking on the next bound towards cross-domain awareness with the incorporation of additional domain awareness 'overlays' will have to address capacity issues such as the infusion or

broadening of personnel competency with cross-domain expertise, balanced against risk of information overload *vis-à-vis* dilution of focus. Until then, overcoming collaborative tensions associated with the collation and sharing of information, mutual sharing of insights into maritime security-related sense-making methodologies/logics, determining baseline information parameters to initiate action-able info-sharing cooperation, within and across national boundaries, to enhance maritime security should be challenge enough.

Conclusion

In a highly globalised world, where the political economy and strategic orientation of many nations are *Merchantalist* maritime, if not *Mahanian* maritime, achieving CMDA may well become a matter of ‘best national interest’ for many trading nations who place a high premium on the unimpeded flow of global commerce and seek to safeguard the global commons for the international shipping community as a universal public good.

While the systems, schemes and modalities of cooperation have yet to be worked out, with many still at an early stage of development and ‘competition’, what has already been envisaged and rolling-out in the pipeline should enable the many interested States, industry and other stakeholders around the world to better appreciate the benefits and opportunities that achieving CMDA represents; albeit balanced against resource commitment and costs involved. This should spur all parties to make the necessary investments and

integration of best systems and practices in “a spirit of partnership”²³ to launch a new era, a maritime renaissance, of unprecedented marine safety and maritime security cooperation that is in the interests of the wider international maritime community as a whole, by actively contributing to the creation of a robust, reliable and resilient CMDA network ... an idea whose time has *finally* come. ☺

(Ed note: The unabridged version of this article is available as RSIS Working Paper No. 141 at <http://www.rsis.edu.sg/publications/WorkingPapers/WP141.pdf>)

Endnotes

- ¹ See Friedrich Nietzsche, *On the Genealogy of Morals and Ecce Homo*, translated by Walter Kaufman & Reginald J. Hollingdale, (New York: Random House, 1969), p119.
- ² The substance is well known as the terrorists’ weapon of choice, and was used in the bombings in Bali in 2002 and Oklahoma City in 1995. See Linton Besser, ‘Explosive Cargoes Steam by Airport’, *Sydney Morning Herald*, 5 Sep 07.
- ³ The NSMS is the pioneering comprehensive maritime strategy for maritime security, created in response to US National Security Presidential Directive-41/Homeland Security Presidential Directive-13. See Wendy Kay, Stephanie McFadden & Matt Lincoln, ‘Global Maritime Integration: A Force Multiplier’, *The ONI Quarterly*, (Jan 2007), pp4-7.
- ⁴ Visit, Board, Search and Seizure (VBSS).
- ⁵ Singapore has embarked on the development of RAHS that encompasses a unique combination of cutting edge concepts, methodologies and technological solutions, and aims to provide policy makers with anticipatory knowledge of the nature of potential upcoming issues so that risks may be minimised and opportunities maximised. This whole-of-government enterprise is done by detecting ‘faint’ signals; networking and linking the various governmental and private agencies; and fostering shared and informed analysis based on methodological diversity. The vision is that “RAHS will empower people with greater foresight to minimise the possibility of strategic surprises”. See Barry Desker cited in Barry Zellen, ‘Mitigating the Dangers of Strategic Surprise: Singapore rises to the occasion with RAHS’ (2 Apr 07),

- available at <http://enterpriseinnovator.com/index.php?articleID=11114§ionID=25>
- 6 As described by Stephen Flynn in a discussion with him in Singapore (27 Aug 07). Stephen Flynn, an ex-USCG officer, is a Jeane F. Kirpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations; he is also author of *The Edge of Disaster: Rebuilding A Resilient Nation*, (New York: Random House, 2007).
 - 7 See speech by Singapore Defence Minister Teo Chee Hean at ground breaking ceremony of Changi Command and Control Centre (27 Mar 97) available at <http://app.sprinter.gov.sg/data/pr/20070327984.pdf>
 - 8 See George Galdorisi & Darren Sutton, 'Achieving the Global Maritime Partnership: Operational Needs and Technical Realities', *RUSI Defence Systems*, (Jun 07) pp68-71.
 - 9 'Indo-US relation is Solid: US Admiral Keating', *ANI* (23 Aug 07).
 - 10 See Christopher P. Cavalas, 'USS HMS Manchester – In Atlantic Exercise with USN, UK ships Take Unprecedented Role', *Defense News*, (6 Aug 07), p4.
 - 11 The Strait of Malacca was the centre of a political storm in 2004 between the waterway's littoral states and US Admiral Thomas Fargo, then Commander-in-Chief, US Pacific Command, who had reportedly announced that under the Regional Maritime Security Initiative, the US was planning to deploy marines and special forces in and around the strait to combat terrorism, proliferation, piracy, gun-running, narcotics-smuggling and human-trafficking. See Vijay Sakhuja, 'Malacca: Who's to pay for smooth sailing?', *Asia Times Online*, 16 May 07. For more on the differing perspectives over this issue, Ary Hermawan, 'Malacca Coast Patrol to Stay Local', *Jakarta Post*, 26 Aug 07 & 'Who Owns the Malacca Straits', *Jakarta Post*, Editorial, 28 Aug 07.
 - 12 See Eric Watkins, 'Obstacles to Closer Counter-Terrorism Coordination in Malacca Straits', *Terrorism Monitor*, Vol.5 No.13 (6 Jul 07), The Jamestown Foundation, pp10-12; also available at <http://www.jamestown.org/terrorism/news/article.php?articleid=2373531>
 - 13 Singapore, Indonesia and Malaysia have in recent years coordinated maritime and air patrols in the Malacca Straits. Pirate attacks in the Malacca Straits, which carries half the world's oil and more than a third of its commerce, have been on the decline since Jul 05, with 11 cases reported in 2006. The improvement in maritime security led to the Loyld's JWC to rescind its declaration which resulted in the imposition of higher insurance premiums for ships transiting through the strait the year before.
 - 14 'See Q & A with RADM Richard Kelly', *ONI Quarterly*, (Jan 07), pp13-15.
 - 15 See Vice Admiral Roberto Cesaretti, 'Combating Terrorism in the Mediterranean', *NATO Review*, (Autumn, 2005), available at <http://www.nato.int/docu/review/2005/issue3/english/art4.html>
 - 16 See interview with Royal Navy's Chief of Naval Operations Admiral Sir Alan West, 'Towards Maritime Domain Awareness', *Asian Defence and Diplomacy*, Vol.13 No.2 (Feb 06), pp18-21.
 - 17 ReCAAP was initiated by the Japanese Government as a multilateral cooperation and agreement initiative among the regional countries to combat piracy and enhance the regional maritime security.
 - 18 The Focal Point is the point of contact for the contracting parties and can either be naval/coast guard personnel or port authorities staff. They assist ISC in the the collection and management of information on piracy & sea robbery incidents within their respective national territorial waters and jurisdiction, dissemination of information with ISC, other Focal Points and their country's shipping community, facilitate investigation for their individual country law enforcement agencies and coordinate with neighbouring Focal Points for surveillance and enforcement actions on piracy & armed robbery against shipping incidents.
 - 19 Irvin Lim, 'Not Yet All Aboard...But Already All At Sea Over Container Security Initiative', IDSS Working Paper No.35 (Singapore, Oct 02), pp1-29; and 'Fireball on the Water: Naval Force Projection-Protection, Coast Guarding, Customs Border Security & Multilateral Cooperation in Rolling back the Global Waves of Terror...from the Sea', IDSS Working Paper No.53 (Singapore, Oct 03), pp1-30.
 - 20 The 2005 Rome Declaration on Illegal, Unreported and Unregulated Fishing adopted by fisheries ministers calls for ensuring all large scale fishing vessels operating on the high seas be required by their Flag State to be fitted with VMS no later than December 2008. See Vessel Monitoring Systems available at <http://www.ffa.int/node/946>; <http://www.fao.org/fi/website/FIRetrieveAction.do?dom=topic&fid=13691>; and <http://www.wcpfc.int/pdf/Conservation%20and%20Management%20Measure-2006-06%20%5BCom mission%20VMS%5D.pdf>
 - 21 For access to *AISLive* website, see <http://www.aislive.com/>
 - 22 For example, the US ONI has developed the Global TRADER cargo analysis tool kit. See Charles Dragonette, 'Fitted for the Voyage: ONI Leads the Way in Global maritime Intelligence Integration', *The ONI Quarterly* (Jan 2007), pp8-12.
 - 23 For more on the need for navies to stay alongside the maritime industry in a spirit of partnership, see Geoffrey Till, *Seapower: A Guide for The Twenty-First Century* (London: Frank Cass, 2004), p103.



LTC Irvin Lim is currently a Branch Head in Naval Intelligence Department. He has served as Commanding Officer of *RSS Vigour* and *RSS Justice*, and was also formerly an Assistant Director with the National Security Secretariat. LTC Lim is a recipient of the SAF Postgraduate Scholarship for a MSc in Strategic Studies from IDSS-NTU (UOB Gold Medal). He also holds a BA (First Class Honours) in Communications Studies from Murdoch University, Perth, Australia (University Medal in the Arts), and a MBA from University of Leicester, U.K. A top Distinguished Graduate of the US Naval War College, he was the first prize winner in CDF Essay Competition 1998.

Building Maritime Security in Southeast Asia

Outsiders Not Welcome?

by MAJ Victor Huang



Today's globalized economy is intricately interconnected and heavily dependent on maritime trade in order to sustain the movement of energy, raw materials, and finished goods. The arteries of global trade include the narrow waterways of Southeast Asia, with about a third of the world's trade and half its oil transiting through the Straits of Malacca and Singapore alone.¹ As China and India continue their strong growth, sea trade through the straits is expected to increase correspondingly.² Major economies such

as the United States, China, Japan, and India all have stakes in ensuring the safe passage of shipping through the region. The littoral states of Southeast Asia may be the most concerned of all; any interruption in shipping would heavily impact their economies by disrupting port operations and the smooth flow of raw materials and finished products. Armed robbery at sea is a persistent problem in the area, and maritime hijackings and kidnappings continue to occur.³ There are fears that the straits could become a target for terrorism

and a haven for illegal trafficking of people and weapons.⁴ Many states are interested in the strengthening of maritime security in Southeast Asia in order to protect their trade and prevent illegal activity.

While the littoral states have recently overcome historical mistrust sufficiently to engage in basic maritime cooperation, the efforts of extraregional players to introduce security frameworks from without have been met with ambivalence or outright rejection. For example, the Regional Maritime Security Initiative (RMSI), proposed by the United States, was strongly criticized after the media incorrectly reported that U.S. high-speed vessels would conduct antiterrorist patrols in the Strait of Malacca;⁵ similarly, the Proliferation Security Initiative (PSI) continues to be viewed with suspicion.⁶ Resistance to the establishment of security frameworks can arise from outside Southeast Asia as well. In 1999, a proposal of the Japanese prime minister, Keizo Obuchi, that a regional coast guard be created as an antipiracy measure was strongly opposed by China.⁷

The resulting absence of extraregional states in operational maritime security initiatives is depriving the region of important resources and capabilities such as information sharing and responsive multinational decision making, which are especially important in view of the multinational nature of maritime trade.⁸ The rejection of outside help by the littoral states is puzzling, since their presence would contribute to the shared goal of improving overall security. Are outsiders simply not welcome in Southeast Asian maritime security cooperation?

This article argues that effective maritime security cooperation in Southeast Asia can be achieved only under a neutral multinational framework. The effort must be largely led and implemented by the littoral states themselves, in order to avoid power rivalries. At the operational level, effective cooperation can be achieved through information sharing and operational coordination between states.⁹ However, the conduct of patrols and enforcement actions within a littoral state's territorial seas must remain the responsibility of that state, in order to protect coastal state sovereignty.

To date, effective operational cooperation has been achieved only under regional agreements that are limited in scope and goals, whereas extraregional efforts have been hobbled by politics. By studying these efforts as case studies and recognizing the issues that inhibit or facilitate regional cooperation, extraregional states can devise strategies to increase their participation in regional security cooperation and apply lessons to promote such international frameworks as PSI and the "thousand-ship navy."

This article evaluates how the willingness of the littoral states to cooperate varies according to differing threat perceptions, concern over sovereignty, and a desire for geostrategic nonalignment. It surveys recent attempts at maritime cooperation and analyzes the factors for success or failure. Finally, the article discusses how extraregional players could contribute toward meaningful maritime security cooperation without causing affront to regional sensitivities.

The Littoral States

We begin by examining the littoral states that border the Malacca and Singapore Straits (see map 1), which is the waterway in the region that has attracted the greatest attention.

Singapore

The city-state of Singapore is heavily dependent on maritime trade to fuel its export-driven economy and its hub status in the transshipment trade and in oil refining. Among the three littoral states, Singapore's economy would be most severely affected by a disruption in the free flow of shipping through the region. Singapore also keenly feels the threat of maritime terrorism. First, its advanced infrastructure — including its container port, its petrochemical refineries, and the city itself — would suffer the greatest economic damage from a terrorist attack. Second, its city center and critical industries are situated on its southern coast adjacent

to the busy Singapore Strait, exposed to possible maritime attack with minimal time and space for reaction should one of the vessels in the busy waterways have hostile intent. This heightens Singapore's desire for advance warning through information sharing. Third, Singapore is an ideologically attractive target because of its close links with Western states, which offend radical religious fundamentalists.¹⁰ This threat environment has heightened Singapore's sense of vulnerability; Teo Chee Hean, Singapore's minister for defense, has consistently maintained that maritime terrorism remains "a clear and present danger."¹¹ A recent article in *POINTER*, the journal of the Singapore Armed Forces, reasoned that terrorist organizations have the "capability, intent and opportunity" to conduct a maritime attack.¹² Singapore is eager to enhance further international and interagency cooperation in order to defend against the threat of maritime terrorism.



Map 1. The Straits of Malacca and Singapore.

Recognizing the importance of maritime security, Singapore has built a modern and capable navy and police coast guard that effectively protect the sixty-mile-long Singapore Strait. In 2003, Singapore established the interagency Maritime and Port Security Working Group, which brings together the navy, police coast guard, and the maritime and port authority. The group implemented regulatory measures to improve port security and control the movement of shipping within the port.¹³ Singapore also monitors the vessels that pass through the Singapore Strait, via its vessel traffic information system.¹⁴ This system uses coastal radars to track up to five thousand vessels; it is integrated with electronic navigational chart displays and synchronized voice, track, and data recording, allowing historical and real-time traffic analysis.¹⁵ Within the region, Singapore is one of the most vocal advocates of international cooperation;¹⁶ it enjoys close ties with regional countries, as well as with the United States, China, and Japan.¹⁷

Malaysia

Like Singapore, Malaysia is dependent on maritime trade. Eighty percent of its trade passes through the Strait of Malacca, and major Malaysian ports are situated on the strait itself. Malaysia is also concerned with protecting its fishing and tourism industries, which would be adversely affected by collisions and groundings and any oil spills that might result. Accordingly, Malaysia is focused on ensuring navigational safety and protecting against environmental threats, in addition to countering piracy.¹⁸ Previously, Malaysian policy makers had downplayed the threat of

maritime terrorism and argued that no proof existed of a “concrete nexus” between piracy and terrorism.¹⁹ Recently, however, Malaysia has warned of the possibility of terrorist attacks using hijacked ships, including those carrying dangerous materials. In June 2007, Malaysia’s top police official stated that maritime terrorism was a “real and possible” threat that could “devastate Southeast Asia’s economic environment and severely disrupt trade.”²⁰ The Malaysian deputy prime minister, Najib Razak, has called for greater vigilance and intelligence sharing to combat piracy and prevent terrorism along the Malacca Strait.²¹

To improve its effectiveness at policing its own waters, Malaysia took the major step of reorganizing its five maritime agencies to form the Malaysian Maritime Enforcement Agency, which was established in May 2004 and officially launched in March 2006. The agency will buy new vessels, refurbish many of its seventy-plus existing craft, and acquire six helicopters for surveillance, enforcement, and search-and-rescue duties.²²

Malaysia contends that the littoral states themselves have the capacity to safeguard the straits. Nonetheless, the Malaysians “find it difficult to accept that while international users consider the straits as an international sea lane which they have the right to use,” the effort and heavy financial cost of securing the strait and ensuring navigational safety are regarded as the responsibility of the littoral states.²³ Therefore, “modalities for burden sharing” should be explored.²⁴ This will become more important in the

future, as traffic volumes are expected to increase. Malaysia is wary, however, of “internationalization” of the strait, which would impinge upon regional security interests.²⁵

Indonesia

Indonesia has a smaller economic stake than Singapore or Malaysia in the safety of the Malacca and Singapore Straits, because the majority of its trade is conducted through the Lombok and Sunda Straits.²⁶ Indonesia’s attention is more focused on such domestic issues as economic development, political reform, territorial integrity, and militant Islamism.²⁷ For the Indonesian navy, countering piracy may also be less important than patrolling its extensive maritime borders, handling maritime border disputes, and countering smuggling, illegal fishing, and environmental degradation.²⁸ Indonesians are particularly sensitive to border disputes after the painful experience of losing two small islands off eastern Borneo, Sipadan and Ligitan, to Malaysia as the result of an International Court of Justice decision in 2002.²⁹ The adjoining oil-rich Ambalat region of the Celebes Sea is still disputed;³⁰ it is highly valued by Indonesia, which sent seven warships and four F-16s there in March 2005 after alleged incursions by Malaysian warships and aircraft.³¹

In addition, Indonesia’s enforcement capacity is stretched by lack of funding and poor maintenance of its ships. According to Indonesian defense minister, Juwono Sudarsono, only 60 percent of Indonesia’s fleet of 124 ships is operational;³² in contrast, the chief of staff of the Indonesian navy, Admiral

Slamet Soebijanto, estimates that at least 302 ships and 170 aircraft are required to protect the nation’s archipelago of seventeen thousand islands.³³ Although Indonesia is acquiring new patrol boats, it has asked the United States for military assistance in the form of training and support in order to build its enforcement capacity.³⁴ Indonesia has stressed, however, that foreign military presence is out of the question.

Indonesia’s incentive to protect the straits is to demonstrate sovereignty over its waters, while promoting good international relations, especially since it receives security assistance and counterterrorism funding from the United States and Australia and aid from Japan.³⁵ Indonesia has also promoted cooperation between the littoral states;³⁶ held biannual coordinated patrols with India since September 2002;³⁷ and signed agreements with Australia, Japan, and India to increase cooperation in security matters, including maritime security. Indonesia also expanded its defense interactions with the United States after the restoration of U.S. international military education and training (IMET), and operational exchanges, such as the annual “Cooperation Afloat Readiness and Training” (CARAT) exercises, were broadened to build understanding and interoperability further. For example, the sea phase of exercise CARAT was lengthened to five days in July 2006, more than double the length of the previous year’s exercise.

Attempts at Regime Building

There have been several efforts to involve the littoral states in maritime cooperation. These efforts can be split

into two types: top-down frameworks proposed by extraregional stakeholders, and bottom-up efforts agreed between the littoral states themselves. These efforts are aimed at shaping the regional maritime security environment, and some states hope that they will result in regional maritime regimes favorable to their interests.

An *international regime* implies “regulated patterns of practice on which expectations converge [that] govern state behavior in specific areas of international relations.”³⁸ There are many maritime regimes that cover the rights of states in the protection of shipping, fishing, marine resources, and other areas. The most comprehensive and important maritime regime today is the UN Convention on the Law of the Sea (UNCLOS). In the Malacca and Singapore Straits, all three littoral states are party to UNCLOS, which specifies the rights and obligations of international strait states in their territorial seas versus the right to transit passage of foreign states.

The idea of a maritime regime is an appealing one. Since the regional states have a common interest in enhancing maritime security, it would be in the national interest of each of them to participate.³⁹ In 1991, Michael Leifer, for example, envisaged a stable and peaceful maritime regime in East Asia whereby states could pursue their interests and manage their resources in accordance with the principles of international law and without the risk of conflict.⁴⁰ While many conferences have been held to improve understanding and build confidence, the region’s states

have been reluctant to move beyond the status quo.⁴¹ Nevertheless, the ideal of building a maritime security regime has remained attractive to the present day, especially for the stakeholders with the most to gain, such as the United States, Japan, and Singapore. The U.S. *National Strategy for Maritime Security*, published in 2005, stated that “regional maritime security regimes are a major international component of this Strategy and are essential for ensuring the effective security of regional seas.”⁴² Let us now survey several initiatives aimed at maritime security regime building, beginning with those initiated by extraregional stakeholders and aimed at direct operational cooperation.

Top-Down Frameworks

Southeast Asia is a region of not only many diverse states but also of overlapping spheres of influence between rival extraregional powers. Attempts by one to introduce a security regime have been rebuffed by others who perceive them as upsetting the regional balance.

Japan’s Ocean Peacekeeping Force concept is an example of an initiative by an extraregional power that was stifled.⁴³ Throughout the 1990s, Japan tried to increase regional cooperation and enhance security by providing much-needed training and assistance to the littoral states. Building upon these efforts, Prime Minister Keizo Obuchi formally proposed, at the Association of Southeast Asian Nations (ASEAN) Plus Three (Japan, South Korea, and China) summit in 1999, the formation of a regional coast guard to combat piracy. It was to be based on multilateral

patrols by forces from Japan, South Korea, China, Malaysia, Indonesia, and Singapore. The proposal was immediately and strongly opposed by China, which saw in it a Japanese move to extend its security role in East Asia and contain Chinese maritime influence.⁴⁴ Subsequent Japanese-proposed initiatives, like the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), have been much less ambitious in scope, covering only voluntary information submission, and funded by voluntary contributions. This episode suggests that, in general, attempts by extraregional powers to exert leadership are likely to trigger unfavorable reactions from rivals. Since the littoral states can ill afford to offend any of the extraregional powers, externally led efforts at leading change are unlikely to meet with success.

Another difficulty faced by externally led efforts is that they may raise sovereignty concerns. This was the situation faced by the Regional Maritime Security Initiative, a conceptual framework proposed by the United States in 2004 for neutral, multilateral maritime security cooperation. RMSI was intended to be a voluntary partnership of regional states to share information and provide cueing (early warning) to counter transnational threats.⁴⁵ Unfortunately, the media incorrectly reported that Admiral Thomas Fargo, Commander U.S. Pacific Command (USPACOM), had testified to Congress on 31 March of that year that American Special Forces and Marines would patrol the Malacca Strait in high-speed vessels.⁴⁶ Although this was untrue, RMSI was permanently tainted by this

misunderstanding, even in academic papers.⁴⁷ RMSI was immediately blasted by the leaders of Malaysia and Indonesia, who condemned the proposed deployment of U.S. forces in the strait as a direct affront to their sovereignty.⁴⁸ (While Chinese analysts wondered whether RMSI was designed to contain China, Chinese officials said little and seemed content to stand aside in this diplomatic fracas.)⁴⁹ As a result of widespread condemnation, USPACOM allowed the RMSI concept to wither away, and “RMSI” vanished from the command’s official communications in 2005.⁵⁰

Even when considered under its true spirit, RMSI would likely not have succeeded. While Admiral Fargo pitched it as a voluntary partnership of the willing, it appeared that the United States would take a leadership role in concept development and implementation. That would have raised fears that it sought to assume the initiative in the region, especially in light of the U.S. history of hub-and-spoke military diplomacy (notably in the organization of the Iraq invasion of 2003). This would surely have provoked the ire of China and other powers. As it happened, no objections were raised, because the issue of U.S. forces stationed in the Malacca Strait proved much more sensitive, and sovereignty concerns in that connection provided a convenient diplomatic “out” for the rejection of RMSI. China was wise to keep silent, because its concerns over American leadership would have seemed insensitive next to the more important issue of sovereignty.

Concern about international law and U.S. leadership was also evident in the region's response to the Proliferation Security Initiative. The PSI is a U.S.-led global initiative to prevent traffic of weapons of mass destruction (WMD). PSI requires the political cooperation of many other countries to succeed; flag-state permission is often necessary for interdiction at sea. PSI is an interesting test case for the region, because it has the appearance of a top-down framework designed to achieve the common goal of nonproliferation, and the obligations of PSI "participants" (as opposed to "members") are recommendatory and legally nonbinding. To emphasize this, PSI is deliberately marketed as an "activity" and not an "organization." Although PSI participants have declared that they are committed to certain principles to impede and stop shipments of WMD, including searching in their waters vessels "reasonably suspected" of carrying such cargoes, they are not obliged to take part in any specific activities that they oppose. Also, they need only "seriously consider" providing consent for their vessels and aircraft to be searched when suspected of carrying WMD. All in all, PSI could be seen as an effort to facilitate operational cooperation and by which participants can signal political support for nonproliferation. It attempts to promote multilateral cooperation without a cumbersome treaty apparatus.⁵¹ In addition, the spirit of PSI was emphatically affirmed by the passage on 28 April 2004 of UN Security Council Resolution (UNSCR) 1540, requiring all states to take measures to prevent proliferation.⁵²



Participants of a PSI maritime interdiction exercise; PSI can be seen as an effort to facilitate operational cooperation and by which participants can signal political support for nonproliferation.

Nonetheless, participation in PSI by Asian states was initially very low. Only Japan and Singapore expressed early public support and formally signed on. Other states might have refrained from participating because of concern about its "ad hoc, extra-United Nations, U.S.-driven nature."⁵³ In September 2004, the Malaysian prime minister, Abdullah Badawi, declared to the UN General Assembly that while Malaysia was committed to nonproliferation, there was a need for multilateral negotiations for "universal, comprehensive and non-discriminatory agreements and arrangements."⁵⁴ This statement reflected fears that American leadership would be nonconsultative and unilateral, that implementation of PSI would "constitute a major shift

from negotiated multilateralism of the post-war system to cooperative unilateralism under post-Cold War American hegemony.”⁵⁵ There were also concerns that the United States would use the Proliferation Security Initiative in an inequitable manner against countries, such as Iran and North Korea, that it designates as “rogue states.”⁵⁶

Some countries cited concern over the legality of the initiative as well. Since the U.S. national security strategy states that the United States will, if necessary, act preemptively against WMD threats, some states are concerned that it would use the PSI to conduct interdictions in ways that violate international law.⁵⁷ In September 2005 China declared that it would not join PSI due to concerns over legality.⁵⁸ In March 2006, Indonesia declined Secretary of State Condoleezza Rice’s request that Indonesia join the PSI.⁵⁹ Subsequently, on 10 June 2006, the Indonesian minister of defense, Juwono Sudarsono, wrote in the *Jakarta Post* that Indonesia would not join PSI because it “contravenes provisions of [UNCLOS].”⁶⁰ He further explained in his official “weblog” that “it was impossible for Indonesia in strictly legal terms to accept the total package of the PSI, as it endorsed interdiction of vessels passing through Indonesia’s territorial waters [as] in the high seas.”⁶¹ In fact, PSI is intended to operate in a manner “consistent with national legal authorities and relevant international law and frameworks.”⁶² This example shows how concern over legality and neutrality can persist even over an initiative that has been deliberately designed to be legal and neutral.

While the Proliferation Security Initiative has had some successes, until very recently it appeared unable to make further inroads into Southeast Asia after its rejection by China and Indonesia.⁶³ American statements aimed at depoliticizing PSI and emphasizing its multilateral, voluntary nature failed to produce new participants in Asia willing to declare their support publicly. Paradoxically, the passage of UNSCR 1540 in April 2004 made open participation in PSI less politically attractive, in that the resolution *requires* states to conduct counterproliferation. Participating in PSI would no longer signal support for counterproliferation in general but support for U.S.-led operational cooperation in particular. This situation was exacerbated by the fact that the founding PSI members were the United States and other Western nations. Following an apparent U.S. lead in an initiative supported by only two states within Asia was something that most regional states, in particular Malaysia and Indonesia, were unwilling to do, as it might have antagonized China.

Many states took the politically expedient option of being a “supporting” country without making a “public statement of support,” as encouraged by the United States.⁶⁴ From 2003 to 2007, such states took part in PSI conferences but their identities were not known.⁶⁵ This situation changed on 1 May 2007, when the United States published a list of participants — eighty-two countries,⁶⁶ this was a staggering increase from the seventeen countries listed in September 2006.⁶⁷ Within Southeast Asia, Brunei,

Cambodia, Papua New Guinea, and the Philippines are now listed by the United States as participants, although they have not made public declarations of support.⁶⁸ It remains to be seen whether the large number of participants will confer an air of neutrality on PSI and pave the way for the recruitment of more participants. Also, the commitment level of these “revealed” PSI supporters remains in doubt in the absence of public statements of support.

Several lessons can be drawn from these three attempts at regime building. First, ambitious attempts at regime building by extraregional powers are unlikely to succeed, because of major-power rivalries. This leads to inaction on the part of regional states who wish to preserve their nonalignment. China’s economic influence in the region and suspicion toward American and Japanese motives in particular will continue to deter smaller states from allowing any of the major powers to play too great a role in regional regime building.

Second, offers of external operational assistance run up against sovereignty concerns related to direct intervention by foreign powers. The littoral states do not wish their waters patrolled by other countries, desiring to prevent major-power rivalries and to retain tight control over their territorial seas. Some of this reluctance can be attributed to enduring postcolonial nationalism and to popular antagonism toward the United States.⁶⁹ Extraregional players should also keep in mind that Indonesia, the world’s fourth most populous country, has historically regarded itself as a regional power and remains fiercely nationalistic.

Third, there is evidence of a strong desire to preserve the status quo under existing international law and of resistance to new precedents that might compromise future actions or negotiations. Thus, Indonesia has taken a “wait and see” stance toward PSI since 2003; while it has declined to become a participant, it has not ruled out partial adherence to PSI provisions on an ad hoc basis, thereby keeping its diplomatic options open without compromising any of its interests.⁷⁰

In summary, if a littoral state is to participate in a formal maritime security regime, it must be prepared to give up some of its political freedom of action in exchange for greater security. At present, the threats are not sufficiently compelling, and the political costs, both foreign and domestic, are too great for Malaysia and Indonesia to do so.

Bottom-Up Building Blocks

An alternative approach to deliberate regime building is to put in place mechanisms or even institutions to perform the tasks necessary for operational cooperation. For example, coordinating patrols and sharing information are relatively simple, unobjectionable actions that can be undertaken by the littoral states among themselves. A long tradition of confidence building through bilateral, coordinated antipiracy patrols, bilateral and multilateral exercises, and personnel exchanges and interactions has built a firm foundation from which the region might progress to noncoalition operational cooperation.⁷¹ An additional benefit of these relatively humble initiatives is that they tend to

originate within the region itself (an exception was ReCAAP, initiated by Japan).

The Malacca Straits Patrols was the first multilateral initiative to be implemented in the region.⁷² It was deliberately designed to be modest, originating from and limited to the three littoral states, and restricted in scope so as to avoid sovereignty issues. The three littoral states, expanding on long-standing bilateral coordinated patrols in order to enhance operational cooperation, launched trilateral coordinated patrols on 20 July 2004.⁷³ Since the sea patrols are coordinated, not joint, each littoral state's force patrols only within its own territorial seas, with no right of pursuit across territorial sea boundaries; the states rely on a hand-off mechanism to handle cross-boundary enforcement. Therefore, they gained in operational effectiveness without the issues of legality that would arise from intrusion into other states' waters. A conceptually linked but officially unrelated boost to the initiative's effectiveness was Project SURPIC, a technical system that allows information sharing between Singapore and Indonesian command and control (C2) centers in order to achieve a common operating picture in the Singapore Strait, facilitating communication and enforcement.

An "Eyes in the Sky" initiative to enhance surveillance by combined maritime air patrols was launched by the littoral states and Thailand on 13 September 2005.⁷⁴ Previously, each state had conducted air surveillance patrols only within its own airspace. This new program allows combined air patrols

across territorial boundaries, allowing for better effectiveness in the narrow straits as well as promoting operational cooperation. A foreign liaison on board each aircraft controls actions over the waters of that officer's state, assuaging concerns over sovereignty and ensuring that states do not abuse the flights for other purposes, such as intelligence gathering. The use of air assets, which have less psychological "presence" than surface craft, also alleviates sensitivity about sovereignty. Since the aircraft can conduct only surveillance, not enforcement — in fact, they carry no weapons that could be used for enforcement purposes — there is no possibility of one state enforcing laws in another state. Overall, such efforts as these have no impact on foreign-power rivalries or international law, and they demonstrate the ability of the littoral states to police their own waters and airspace under initiatives limited in scope and purpose.

Similarly, working under the principles of regional inclusiveness, neutrality and noninterference, Japan managed to refashion its Ocean Peacekeeping (known as OPK) concept into the more conservative and ultimately successful ReCAAP proposal made by Prime Minister Junichiro Koizumi in 2001. ReCAAP is a broadly based initiative, involving all the ASEAN nations plus Bangladesh, China, India, Japan, South Korea, and Sri Lanka.⁷⁵ ReCAAP, which came into force on 4 September 2006, is "the first regional government-to-government agreement to promote and enhance cooperation against piracy and armed robbery at sea in Asia."⁷⁶

The operational heart of ReCAAP is its Information Sharing Centre (ISC), located in Singapore, which reports and coordinates responses to incidents at sea. The member states also agree to cooperate in capacity building, legal assistance, and extradition.

The establishment of ReCAAP was a breakthrough. It is an international institution to fight piracy, not merely a set of multilateral arrangements and exercises. The inclusion of regional powers such as China, India, Japan, and South Korea and the basing of the ISC in a littoral state have also given the initiative neutrality and inclusiveness. Malaysia and Indonesia have not yet ratified the agreement, though they are expected to do so.⁷⁷ Their hesitation is attributed to concern over the location of the ISC in Singapore;⁷⁸ this concern, in turn, reflects rivalry between the littoral states, as well as fear that the ISC would publish reports unfair to other member states.⁷⁹ This delay suggests that the neutrality of such initiatives is important not just between powers but also between the littoral states themselves.

On 27 March 2007, Singapore announced that it would construct a command and control center to “house the Singapore Maritime Security Centre (SMSC), an Information Fusion Centre (IFC), and a Multinational Operations and Exercise Centre (MOEC).”⁸⁰ The IFC will facilitate information fusion and sharing between “participating militaries and agencies,” and the MOEC will provide the infrastructure for multinational exercises, maritime

security operations, and humanitarian assistance and disaster relief should the need arise.⁸¹ In essence, Singapore is offering a readymade capability that can be leveraged for regional cooperation at any time. This will allow a rapid operationalization of cooperation initiatives should the political environment be conducive. Singapore’s action could also reflect the hope that the existence of an additional C2 facility will spur international cooperation. While it is still too early to see the impact of Singapore’s announcement, Singapore’s command and control center looks to be an important seed crystal for future cooperation when it becomes operational in 2009.



At the launch of Singapore’s Changi C2 Centre; the facility will allow a rapid operationalization of cooperation initiatives should the political environment be conducive.

Toward Win-Win Solutions

When it comes to maritime security cooperation in Southeast Asia, are outsiders not welcome? The evidence shows that extraregional stakeholders *are* welcome in Southeast Asia. The littoral states appreciate the assistance of outside states — but only within limits that are highly circumscribed and not politicized. The region is unreceptive to regime building that sets off power rivalries and sovereignty concerns. In contrast, the efforts of the littoral states themselves have been more modest in scope, characterized by bottom-up cooperation that incrementally builds operational cooperation.⁸² This cooperation has been facilitated by the absence of an overarching framework, which would be political baggage. ReCAAP, for its part, was successful only because it was seen by extraregional powers as neutral and was limited to operational information sharing and low-level, nonmilitary assistance.

Such experience suggests several options extraregional states could take to strengthen regional maritime security. These are in line with the need for multilateralism and neutrality. First, they can share ideas and build understanding through multilateral forums. The annual Shangri-La Dialogue in Singapore, attended by defense ministers, has proved useful for exchanging viewpoints and building understanding.⁸³ The Western Pacific Naval Symposium is similarly valuable at the operational level. Second, they can support intraregional initiatives. Support of such existing initiatives as ReCAAP would improve the prospects for security. Although the United States

is not a member of ReCAAP, it can assist that effort by not establishing parallel or competing initiatives. Singapore's new C2 center is also a possible nexus for future multilateral cooperation.

Extraregional powers can promote confidence and increase interoperability through exercises. Bilateral and multilateral exercises build the operational expertise of local navies, improving their ability to secure the straits. Such exercises also increase interoperability, which would facilitate future operational cooperation should the opportunity arise. These exercises include CARAT and SEACAT between the United States and Southeast Asian navies, and the Five Power Defence Arrangements exercises between the United Kingdom, Australia, New Zealand, Malaysia and Singapore.¹ PSI exercises and discussions should continue to be inclusive in order to build understanding of that initiative.

They can offer technical assistance to build capacity. Such help is welcome in the region, especially by Indonesia.⁸⁴ Outside assistance would render Indonesia, with its limited budget and other priorities, better able to promote maritime security. Japan has installed navigational aids in the Malacca Strait and, through the Nippon Foundation, donated a training ship to Malaysia in June 2006.⁸⁵ While such assistance is not multilateral in nature, it takes place within normal bilateral frameworks, and outside powers have not protested such interactions; political sensitivities

¹ SEACAT (Southeast Asia Cooperation against Terrorism) promotes information sharing and multinational cooperation in maritime interception scenarios.

can also be somewhat lessened by rendering the assistance in low-key, behind-the-scenes ways. Goodwill can also be built through humanitarian civic assistance. Political and operational payoffs accrued to the United States, Japan, and other nations from the tsunami humanitarian relief mission in northern Indonesia, and humanitarian civic assistance should be continued in peacetime.⁸⁶ Humanitarian aid does not directly strengthen regional maritime security, but it can promote mutual understanding and goodwill.

Finally, external powers can work through international organizations. New international frameworks established through the UN and International Maritime Organization would be the most effective way of introducing new norms to the region. Security Council resolutions are difficult to bring to adoption, but the legal authority of such resolutions and the moral authority arising from such focused expressions of international opinion make them highly effective. For example, many of the goals of the Proliferation Security Initiative, as we have seen, were achieved with the passage of UNSCR 1540. In this regard, ratification by the United States of the UN Convention of the Law of the Sea would increase the legitimacy of that vehicle and facilitate the success of future initiatives.

There has been considerable progress in international understanding and cooperation in Southeast Asia. The norms for acceptable participation by outside actors in the region have become more clearly defined through the region's experience with OPK, RMSI, PSI, and

ReCAAP. Future cooperation initiatives can thereby be tailored to avoid regional sensitivities. Although the main focus of such initiatives has been the Malacca and Singapore Straits, the inclusion of Thailand in combined air patrols and the establishment of ReCAAP, involving sixteen countries, suggest a potential to increase the geographical scope of regional cooperation. Ultimately, extraregional players need to appreciate the differing needs and preferences of the littoral states and other extraregional powers and to act accordingly to find a win-win solution for all parties. ☺

Acknowledgements

The author wishes to thank Professor Peter Dutton of the U.S. Naval War College for his help as course paper advisor; and Mr. and Mrs. Gilson B. Gray III for generously sponsoring the Zimmerman-Gray Naval Staff College International Prize, which is dedicated to the memory of their fathers, Commander Donald S. Zimmerman, Jr., USN, and Commander Gilson B. Gray, Jr., USNR, both of whom were Navy pilots.

(Ed note: This article originally appeared in the Naval War College Review, a publication of the U.S. Naval War College, and is reprinted by courtesy of the Review.)

Endnotes

- ¹ *The National Strategy for Maritime Security* (Washington, D.C.: White House, 2005), p15, www.whitehouse.gov/homeland/maritime-security.html.
- ² Teo Chee Hean (speech at RSN fortieth anniversary and commissioning of *RSS Formidable* at Changi Naval Base, Singapore, 5 May 2007).
- ³ According to the International Maritime Bureau of the International Chamber of Commerce, the annual rates of reported piracy incidents in the Malacca Strait have varied over the years: sixteen in 2002, twenty-eight in 2003, thirty-eight in 2004, twelve in

- 2005, and eleven in 2006. These rates have been falling in recent years and the level of violence has decreased, but it is too early to conclude that they would continue to trend downward. Also, there is concern that pirates will resort to “more violent and sophisticated operations.” Jane Chan and Joshua Ho, “Piracy and Armed Robbery against Ships,” *RSIS Commentaries*, 21 March 2007, p2, available at www.rsis.edu.sg/publications/Perspective/RSIS0182007.pdf.
- ⁴ See Catherine Zara Raymond, “The Malacca Straits and the Threat of Maritime Terrorism,” *Power and Interest News Report*, 24 August 2005, www.pinr.com.
- ⁵ John F. Bradford, “The Growing Prospects for Maritime Security Cooperation in Southeast Asia,” *Naval War College Review* 58, no. 3 (Summer 2005), p75.
- ⁶ David Rosenberg, “Dire Straits: Competing Security Priorities in the South China Sea,” *Japan Focus*, 13 April 2005.
- ⁷ Donald E. Weatherbee, *International Relations in Southeast Asia: The Struggle for Autonomy* (Lanham, Md.: Rowman and Littlefield, 2005), p175. The term “piracy” will be used to refer broadly to piracy in international waters as well to as acts of armed robbery within territorial seas. However, strictly speaking, under UNCLOS definitions, piracy takes place only on the high seas.
- ⁸ The situation improved recently when the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) entered into force in September 2006. Malaysia and Indonesia have signed but have not yet ratified the agreement.
- ⁹ In addition, useful cooperation can be achieved between governmental agencies, such international organizations as the International Maritime Organization, and the shipping industry. These modes of cooperation will not be discussed in this article.
- ¹⁰ These fears proved well founded in 2003, when local members of the terrorist group Jemaah Islamiyah were caught plotting bomb attacks on American sailors on shore leave and small-boat attacks on U.S. warships transiting off Changi.
- ¹¹ Teo Chee Hean (speech at groundbreaking ceremony for the Changi Control and Command Centre, Changi Naval Training Base, Singapore, 27 March 2007). This phrase was also used in Teo’s previous speeches.
- ¹² Serene Chua, “Maritime Security: Possibilities for Terrorism and Challenges for Improvement,” *POINTER* 32, no. 2 (2006), pp31–32.
- ¹³ *Ibid.*, p33.
- ¹⁴ *Ibid.*
- ¹⁵ Maritime and Port Authority of Singapore, “Safety & Environment: Introduction,” *Building an International Maritime Center*, www.mpa.gov.sg/safetyenvironment/intro/intro.htm.
- ¹⁶ Singapore has been vocal in urging the region to “move beyond principles” in terms of military cooperation. For example, in 2005 Singapore’s defense minister, Teo Chee Hean, expressed the nation’s interest in introducing joint military activities under the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) umbrella (Robert Karniol, “Singapore Calls on Allies to ‘Move beyond Principles.’” *Jane’s Defence Weekly*, 15 June 2005). In January 2007, Singapore hosted the first ARF maritime-security shore exercise (“Singapore Hosts First Ever ASEAN Regional Forum Maritime Security Shore Exercise,” *Ministry of Defence, Singapore*, 23 January 2007, www.mindef.gov.sg/imindef/).
- ¹⁷ Notably, it was the first country within ASEAN to conclude, in 2003, a free-trade agreement with the United States, which was in part a reward for its partnership in the war on terrorism. Weatherbee, *International Relations in Southeast Asia*, p37.
- ¹⁸ Dato’ Sri Mohd Najib Tun Abd Razak, “The Security of the Straits of Malacca and Its Implications to the South East Asia Regional Security” (speech, Seoul, 13 March 2007), available at www.pmo.gov.my/WebNotesApp/.
- ¹⁹ *Ibid.*
- ²⁰ Agence France-Presse, “Experts Warn of Terrorism, Piracy in Malacca Straits,” 13 June 2007, www.taipetimes.com/.
- ²¹ Agence France-Presse, Bernama, “Share Data to Fight Piracy: Najib,” 3 September 2007, www.straitstimes.com/.
- ²² *DefenseNews*, “Malaysia’s MMEA to Acquire Air Assets,” 5 February 2007, p18.
- ²³ Najib, “The Security of the Straits of Malacca.”
- ²⁴ According to UNCLOS Article 43, “User States and States bordering a strait *should by agreement* [emphasis added] cooperate: (a) in the establishment and maintenance in a strait of necessary navigational and safety aids or other improvements in aid of international navigation; and (b) for the prevention, reduction and control of pollution from ships.” However, according to Article 38, the right of transit passage through international straits cannot be infringed upon by coastal states. Therefore, there is no legal obligation for user states to engage in burden sharing, and participating in such initiatives would set an uncomfortable precedent that might encourage other international strait states to demand burden-sharing agreements also. At present, the subject is under study and negotiation. The Nippon Foundation has limited its appeals for burden sharing to voluntary contributions, stating, “Shipping companies and other users should recognize their corporate social responsibility toward the promotion of navigational safety and environmental protection of the Straits and voluntarily provide the necessary assistance

- to the littoral States.” See Agence France-Presse, “Malaysia Urges Burden-Sharing to Protect Malacca Strait,” 13 March 2007, available at bpms.kempen.gov.my/.
- 25 Najib, “The Security of the Straits of Malacca.” This point is also made in Yoichiro Sato, “U.S. and Japan in the Malacca Strait: Lending Hands, Not Stepping In,” *GloCom Platform: Japanese Institute of Global Communications*, 13 July 2004, www.glocom.org/debates/20040713_sato_us/index.html.
- 26 Barrett Bingley, “Security Interests of the Influencing States: The Complexity of Malacca Straits,” *Indonesian Quarterly* 32, no. 4 (December 2004), p362.
- 27 A fledgling democracy formed after the downfall of General Suharto’s authoritarian government in May 1998, followed by the fall of three presidents through 2004, Indonesia is still struggling to recover from decades of corruption and policy stagnation. Weatherbee, *International Relations in Southeast Asia*, pp30–31.
- 28 Stefan Eklöf, “Piracy in Southeast Asia,” *IIAS Newsletter* 40 (Spring 2006), p29. Indonesia has sent patrol ships to prevent border crossings from independent East Timor into Indonesian-held West Timor (Xinhua, “Indonesian Warships Still Patrolling Border Waters with Timor-Leste,” 7 June 2006, available at english.people.com.cn/). Indonesian patrol ships also patrol its maritime border with Australia, to prevent Indonesian fishing vessels from infringing into Australian waters (“Indonesian Navy Send Two War Ships to Patrol Boundary Near Australia [sic],” *AntaraNews*, 27 January 2006, www.antara.co.id/).
- 29 Azhar Ghani, “Jakarta Using S’pore, KL as Bogeymen?” *Straits Times*, 17 March 2007, available at app.mfa.gov.sg/. (“KL” refers to Kuala Lumpur, the capital of Malaysia)
- 30 See “Malaysia Minister Denies He Apologized over Ambalat,” *AntaraNews*, 30 March 2007, www.antara.co.id/.
- 31 Bill Guerin, “Sulawesi Sea Row Dredges Up Defenses,” *Asia Times Online*, 9 March 2005, www.atimes.com/.
- 32 Coordinating Ministry for Economic Affairs, Republic of Indonesia, “Trade and Investment News,” 24 July 2006, www.jjc.or.id/picture/10332006133543TIN20060724.pdf.
- 33 Agence France-Presse, “Tsunami Opens Door for Normalization of US-Indonesia Military Ties,” 13 February 2005, www.channelnewsasia.com/.
- 34 Ibid.
- 35 Frederick Chew, *Piracy, Maritime Terrorism and Regional Interests*, Geddes Papers (Canberra: Australian Defence College, 2005), p78.
- 36 Indonesia helped to institutionalize the trilateral MALSINDO Malacca Strait coordinated patrols in July 2004, taking in late 2004 the positive step of inviting Thailand to join. Ibid.
- 37 “RI, Indian Navies Conducting Coordinated Patrols in Andaman Sea,” *PR Newswire*, 20 March 2007, available at www.zibb.com/.
- 38 Sam Bateman, “Maritime ‘Regime’ Building,” in *The Best of Times, the Worst of Times: Maritime Security in the Asia-Pacific*, ed. Joshua Ho and Catherine Zara Raymond (Singapore: World Scientific, 2005), p263.
- 39 Arthur Stein, “Coordination and Collaboration: Regimes in an Anarchic World,” in *Neorealism and Neoliberalism: The Contemporary Debate*, ed. David A. Baldwin (New York: Columbia Univ. Press, 1993), pp309–11.
- 40 Michael Leifer, “The Maritime Regime and Regional Security in East Asia,” *Pacific Review* 4, no. 2 (1991), pp126–36.
- 41 Mark Valencia, “Regional Maritime Regime Building,” *Ocean Development and International Law* 31 (2000), p241.
- 42 *National Strategy for Maritime Security*, p15.
- 43 Weatherbee, *International Relations in Southeast Asia*, p175.
- 44 Ibid.
- 45 “Regional Maritime Security Initiative,” U.S. *Pacific Command*, 21 June 2004, available at web.archive.org/web/20051018030410/www.pacom.mil/rmsi/.
- 46 Bradford, “Growing Prospects for Maritime Security Cooperation in Southeast Asia,” p75.
- 47 For example, the account of RMSI in Weatherbee’s *International Relations in Southeast Asia* reflects this misunderstanding. For an example media report, see “Crack U.S. Troops may Be Used to Flush Out Terrorists in Key Southeast Asian Waterway,” *Channel NewsAsia*, 5 April 2004, available at web.archive.org/web/20040405202704/www.channelnewsasia.com/.
- 48 C. S. Kuppaswamy, *Straits of Malacca: Security Implications*, Paper 1033 (India: South Asia Analysis Group, 18 June 2004), available at www.saag.org/papers11/paper1033.html.
- 49 Denny Roy, *Lukewarm Partner: Chinese Support for U.S. Counter-Terrorism in Southeast Asia* (Honolulu, Hawaii: Asia-Pacific Center for Security Studies, March 2006).
- 50 A search of Commander, USPACOM’s speeches shows no references to RMSI after 2004, and its RMSI (www.pacom.mil/rmsi/) website has been removed. According to Archive.org, the site was last accessible in October 2005.
- 51 Mark R. Shulman, *The Proliferation Security Initiative as a New Paradigm for Peace and Security* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, April 2006), p8.
- 52 Henry Low, “The Proliferation Security Initiative Dilemma: To Join or Not to Join?” (research paper, U.S. Naval War College, Naval Staff College, Newport, R.I., 10 May 2005), p8.
- 53 Mark J. Valencia, “Is the PSI Really the Cornerstone of a New International Norm?” *Naval War College Review* 59, no. 4 (Autumn 2006), p128.

- ⁵⁴ Abdullah bin Haji Ahmad Badawi (address at General Debate of the fifty-ninth session of the General Assembly of the United Nations, New York, 27 September 2004).
- ⁵⁵ Rosenberg, "Dire Straits."
- ⁵⁶ Mark J. Valencia, *The Proliferation Security Initiative: Making Waves in Asia*, Adelphi Paper 376 (London: International Institute for Strategic Studies, October 2005), p69.
- ⁵⁷ *The National Security Strategy of the United States of America* (Washington, D.C.: White House, 2006).
- ⁵⁸ Center for Nonproliferation Studies, Monterey Institute of International Studies, "Proliferation Security Initiative (PSI)," *Inventory of International Nonproliferation Organizations and Regimes*, 28 September 2006, cns.miis.edu/pubs/inven/index.htm.
- ⁵⁹ Ibid.
- ⁶⁰ Yuwono Sudarsono [sic], *Jakarta Post*, opinion, 10 June 2006, available at www.thejakartapost.com/.
- ⁶¹ Juwono Sudarsono, "US Secretary of Defense," *Juwono Sudarsono: Integrity in the Strict Sense*, 13 June 2006, www.juwonosudarsono.com/.
- ⁶² Office of the Press Secretary, White House, "Proliferation Security Initiative: Statement of Interdiction Principles," available at www.state.gov/t/isn/rls/fs/23764.htm.
- ⁶³ PSI has been successful in that the major flag states and all the permanent members of the UN Security Council, except China, are full participants. UNSCR 1540 was also a spin-off success from the general acceptance of PSI, as it encapsulates many PSI principles, except for the authorization of maritime interdiction, which was opposed by China. Indonesia, although it would not join PSI, is sympathetic to its aims. President Susilo Bambang Yudhoyono has assigned the chief security minister, Widodo Adi Sutjipto, to study the possibility of undertaking PSI provisions on a partial and ad hoc basis. Juwono Sudarsono, "US Secretary of Defense."
- ⁶⁴ See Valencia, "Is the PSI Really the Cornerstone of a New International Norm?" and Bureau of Nonproliferation, "Proliferation Security Initiative Frequently Asked Questions (FAQ)," *U.S. Department of State*, 26 May 2005, www.state.gov/t/isn/rls/fs/46839.htm.
- ⁶⁵ Valencia, "Is the PSI Really the Cornerstone of a New International Norm?"
- ⁶⁶ Bureau of International Security and Nonproliferation, "Proliferation Security Initiative Participants," *U.S. Department of State*, 1 May 2007, www.state.gov/t/isn/c19310.htm.
- ⁶⁷ Sharon Squassoni, *Proliferation Security Initiative (PSI)* (Washington, D.C.: Congressional Research Service, 14 September 2006), p2, available at www.fas.org/sgp/crs/nuke/RS21881.pdf. Although it was known that other states had publicly declared themselves PSI participants, for a total of more than twenty, the Department of State's PSI website was not updated, resulting in
- some confusion over the actual number.
- ⁶⁸ Bureau of International Security and Nonproliferation, "Proliferation Security Initiative Participants."
- ⁶⁹ According to the Pew Global Attitudes Project report of 13 June 2006, favorable opinions of the United States among Indonesians had fallen from 36 percent to 30. In comparison, Indonesians hold generally favorable opinions of other major nations, such as Germany (56 percent), France (52 percent), Japan (78 percent), and China (62 percent). *Pew Global Attitudes Project*, pewglobal.org/reports/.
- ⁷⁰ In the *Jakarta Post* of 10 June 2006, the Indonesian defense minister wrote, "On June 7, President Susilo Bambang Yudhoyono merely requested that Chief Security Minister Widodo, Foreign Minister Hassan Wirajuda and I consider the possibility of Indonesia's partial and ad hoc adherence to the PSI on a case by case basis, within the framework of maintaining Indonesia's legal sovereignty over its land, territorial waters and airspace."
- ⁷¹ Exercises include the three annual bilateral events undertaken between the three littoral states (Malaysia/Indonesia, Malaysia/Singapore, Indonesia/Singapore), as well as multilateral interactions such as the Five Power Defence Arrangements (Malaysia, Singapore, the United Kingdom, Australia, and New Zealand) and Western Pacific Naval Symposium exercises.
- ⁷² The term "Malacca Straits" was introduced as a verbal shorthand in such initiatives as "Malacca Straits Security Initiative" and "Malacca Straits Patrols" to mean the Straits of Malacca and Singapore.
- ⁷³ The Indonesia-Singapore Co-ordinated Patrol was started in 1992. Also see "Launch of Trilateral Coordinated Patrols — MALSINDO Malacca Straits Coordinated Patrol," *Ministry of Defence, Singapore*, 20 July 2004, www.mindef.gov.sg/.
- ⁷⁴ "Launch of Eyes in the Sky (EiS) Initiative," *Ministry of Defence, Singapore*, 13 September 2005, www.mindef.gov.sg/.
- ⁷⁵ As of the time of writing, all the nations had ratified the agreement except for Malaysia and Indonesia.
- ⁷⁶ Singapore Ministry of Foreign Affairs, "Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)," press release, 4 September 2006, available at app.mfa.gov.sg/.
- ⁷⁷ Vijay Sakhujia, "Regional Cooperation Agreement on Anti-Piracy," *Strategic Trend IV*, 10 July 2006.
- ⁷⁸ Ibid.
- ⁷⁹ John Bradford, *Southeast Asian Maritime Security in the Age of Terror: Threats, Opportunity, and Charting the Course Forward*, Working Paper 75 (Singapore: Institute of Defence and Strategic Studies, April 2005), pp8–9.

⁸⁰ According to a press release, “The Changi C2 Centre will advance multi-agency co-operation and interoperability amongst national maritime agencies, to enhance Singapore’s maritime security capabilities. The Centre will also enable international cooperation and inter-operability between countries to promote maritime security in the region.” “New Maritime Command and Control Centre at Changi,” *Ministry of Defence, Singapore*, 27 March 2007, www.mindef.gov.sg/.

⁸¹ *Ibid.*

⁸² For example, the trilateral coordinated patrols and combined air patrols are relatively simple and were implemented in a step-by-step, task-by-task manner. First, surface patrols were coordinated to improve response. Air surveillance was then added, to improve surveillance.

⁸³ The countries represented at the 2007 Shangri-La Dialogue were Australia, Bangladesh,

Brunei, Cambodia, Canada, China, France, Germany, India, Indonesia, Japan, Malaysia, Mongolia, Myanmar, New Zealand, Pakistan, the Philippines, the Republic of Korea, Russia, Singapore, Sri Lanka, Thailand, Timor-Leste, the United Kingdom, the United States, and Vietnam.

⁸⁴ Indonesia has accepted American and Japanese military and technical assistance and has been reinstated on the U.S. International Military Education and Training program.

⁸⁵ James L. Huffman, “The Nippon Foundation Donates Training Ship to Malaysia,” *Nippon Foundation*, 1 June 2006, www.nippon-foundation.or.jp/.

⁸⁶ For the U.S. tsunami response and the goodwill that resulted, see Bruce A. Elleman, *Waves of Hope: The U.S. Navy’s Response to the Tsunami in Northern Indonesia*, Newport Paper 28 (Newport, R.I.: Naval War College Press, February 2007).



MAJ Victor Huang is the Commanding Officer of the patrol vessel *RSS Resilience*. A Naval Officer by training, he was formerly a Staff Officer in Naval Plans Department and served several tours onboard the missile corvette *RSS Victory*. MAJ Huang is a SAF Overseas Scholar and holds a Bachelor of Science with honours from the California Institute of Technology, with majors in Chemistry and Engineering & Applied Science. He is a recent graduate of the U.S. Naval Staff College in Newport, Rhode Island, where the course paper upon which this article is based won first prize in the Zimmerman-Gray International Essay Competition.

Network Enabled Capability – Dream or Reality?

by Commodore(Ret) Patrick Tyrrell



The Dream

Admiral Nelson was, by any standards, one of the greatest naval commanders who ever lived. Although there is no evidence that he ever visited Singapore, he would, I am certain, have approved of the manner in which the Singapore Armed Forces approach innovation and lateral thinking. His great strength lay in the absolute trust that existed between him and his captains – he trusted them to use their initiative in discharging their respective roles in the battle, valuing innovative ideas, listening to their counsel and, as a result, they had absolute faith in this diminutive Admiral.

Clearly, good leaders can make the difference between disaster and victory. There has long been a debate about how such leaders are made; are they born great or do they achieve greatness through training and experience? In a definitive study of the British military, Norman Dixon demonstrated how personal prejudices and ambitions affect the effectiveness of commanders.¹ I am not intending to enter that debate today; suffice it to say that great leaders are defined in hindsight as they take the right decisions at the right time. Sometimes, those decisions may appear obvious at the time they were taken, more likely however, the decision might

have been seen as risky and uncertain when made until time and events proved it to have been correct.

To those who set policy, grand and eloquent statements make for good copy. Network-Centric Warfare (NCW) or its UK counterpart, Network Enabled Capability (NEC), is full of such “buzz words”; *decision superiority*, *shared situational awareness*, *information exploitation* are but a few of the key principles laid down in explaining the nature of the policy. In the US, where the Revolution in Military Affairs (RMA) initially caught the attention and enthusiasm of the policy makers and the politicians, and in the UK, the concept was seen to provide a way forward through the complexity of realignment following the collapse of the former Soviet Union and the military and strategic imperatives of the Cold War.

The UK’s approach to NEC is set out in JSP 777 edition 1². It is a clear and lucid statement of the need for such an approach. It makes the point that networks have always played a part, at times revolutionary, and cites the example of the network of Roman roads which allowed for a much greater geographical spread of command. However, it fails to point out that those very roads that allowed the Roman command and control to be exercised effectively at long distances from headquarters, also provided the access for the marauding bands of Goths, Visigoths and other barbarians to strike quickly at the very heart of the Roman empire! NEC is expected to deliver the ability “to do better things” rather than “to do things better”. This will reflect that:

- A robustly networked force improves information sharing.
- Information sharing enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronisation, and enhances sustainability and speed of command.
- These, in turn, dramatically increase mission effectiveness.

I am sure that most people within the military information arena will be extremely familiar with the “network” picture, linking land, sea and air assets with the operational and strategic headquarters. The concept is simple: all elements of the national or coalition environment should share information. It is the bedrock of the principles of flexibility of forces and rapid manoeuvrability. The principle of information centric command and control has been around for over a decade. Billions of dollars have been spent trying to deliver the core capability and yet, in a speech at the USAF IT Conference, General Lance Smith stated: “Our legacy systems just don’t talk to each other and the reason for that is that someone thought that there was data that was unique to them. We have to build a culture that is gathering that kind of information and making it available to commanders in the field.”³

In an attack on the inefficiency of the Department of Defense and system integration providers, he said, “I cannot begin to tell you how much of that \$18 billion (referring to the costs of reconstruction in Iraq) was spent on just trying to get systems to talk to one another”.

In those heady days of the Revolution in Military Affairs, much was made of the “new paradigms”, how things were going to be very different from the ways in which we had conducted business in the Cold War. Clearly, the transformation of information processes and communications technology did indeed revolutionise many aspects of military doctrine. One thing it cannot change though is the behaviour of the human element, for example the requirement to adhere to the principles of command. These have been identified by long and bloody history in warfare. Variouslly stated, they include the need for clear objectives, unity of command, economy of force, surprise, morale, simplicity, etc.

We now have the ability to transfer terabytes of data. This is equivalent to the entire contents of the British Library, far more information than human beings can assimilate in a lifetime of study, let alone in the heat of battle. We need, therefore, to be discriminatory, to filter data such that only those likely to be required by a commander is provided to him. It is highly instructive to look at the information requirements of a submarine on patrol. The commanding officer will not wish to compromise his security either by transmitting or by leaving his masts up in order to receive vast quantities of data. This implies that submarines will not be a permanent feature of the net but will join and leave as operational imperatives dictate. We shall return to this issue shortly.

Decision-making by commanders, at whatever level they are operating, has at least two essential aspects.

The first is content of the information needed to make an informed decision and the second is the time within which any decision can be effected. There is inevitably a balance between the information requirements and the speed at which the decision needs to be made. Any mechanism to support effective decision-making must include both the temporal and content aspects of the data.

The Reality

In the twenty or so years that we have enjoyed sophisticated and widespread computer systems, the cost of both the hardware and the software has plummeted and yet the total costs have mushroomed. The reason for this apparent paradox is the requirement to “normalise” large quantities of data which is usually done by employing people to re-enter data that is contained in a legacy system into the new system. As General Lance Smith observed, this costs vast sums of money and rarely delivers effect.

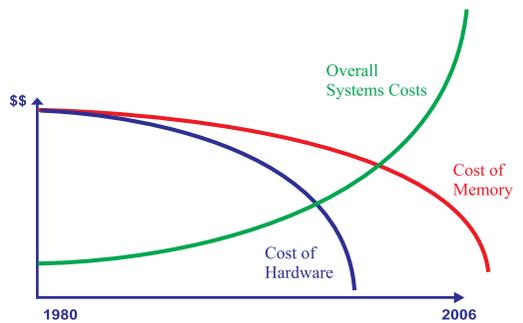


Figure 1. Cost of Computing.

I find it extremely useful to conduct a traditional SWOT analysis (strengths, weaknesses, opportunities and threats) for this capability that will allow us to see where the main advantages lie:

Strengths	Weaknesses
<ul style="list-style-type: none"> • More immediate C2 • Wider sharing of key data • Effective joint and coalition operations • More effective “push/pull” of data 	<ul style="list-style-type: none"> • Can give undue credibility to false data • Information overload vitiates effective decision-making • Focus on systems rather than people • Underlying legacy systems are difficult to access • Decision delay as commander awaits more information
Opportunities	Threats
<ul style="list-style-type: none"> • Greater agility through information sharing • Faster response • Shared vision • Better decision-making 	<ul style="list-style-type: none"> • Enemy action targeted against network • Possibility of deception • Tendency to accept data passively • Ability of senior commanders to be seduced by preconceptions

One solution is to develop a common data dictionary so that wherever data resides, it will do so in a commonly accepted form and be readily exchangeable into other systems. In many ways, this is the data equivalent of *Esperanto*, the universal language. People are essentially different, culturally, socially and behaviourally. Such a dictionary can only work if there is 100% agreement on terms and definitions. When we note that an ape’s DNA is 95% identical to that of a human, we realise that the remaining 5% makes all the difference! Achieving 100% conformity will be extremely difficult, particularly as new applications emerge that demand new definitions.

Modern military doctrine requires far greater flexibility than was historically the case. To develop information processes that allow for the agility of command and control, we need a more sophisticated and intuitive way of looking at the data; a way independent of the original applications, but one that

maintains the integrity and traceability of the information. Agility of command – that ability to be able to shift operational objectives as the wider picture dictates – requires flexibility of the information management to support the commander in the decisions he must take. To do so effectively, he must understand where the information resides and how to access it. He needs to recognise that some information is more accurate than others and be able to discriminate when assessing an operational situation.

A key attribute, often neglected in peacetime military forces, is the ability of a good commander “to think out-of-the-box”. It is difficult to train potential leaders to act as mavericks – to go against established doctrine and to push against the boundaries of that which is established and agreed. One four-star American Admiral remarked: “Senior officers micromanage leaving subordinates to second guess.” One way to encourage tactical innovation is to give subordinates clear objectives but

allow them the freedom to develop their own ways of achieving them. Failures will occur as these subordinates work out tactics that might work and reject those that may not. Such failures should be welcomed as part of the learning experience. Too often, in a competitive world, failure in one area marks out a junior officer as unfit for promotion. Such a policy is not only short-sighted, it is dangerous, as only those officers who never make a mistake by never taking risks will, ultimately, rise to the top.

In looking at NEC, we have focused on the decision maker, the individual who must take ultimate responsibility for his or her actions. We can develop these skills by effective training, both in the classroom and on the ground. The use of artificial environments and sophisticated simulation can reproduce the pressures of command and allow individuals to develop core skills. The technology of NEC, providing a holistic information environment, can be a vital tool in giving that decision maker the key information in time for him to make the appropriate decision.



British troops in Iraq; in looking at NEC, we have to focus on the decision maker, the individual who must take ultimate responsibility for his actions.

It is instructive to look at General Eisenhower’s behaviour in June 1944 as he was about to take one of the most critical decisions of his life – to launch the D-Day landings on the coast of Normandy, France. The weather had been poor and his troops were waiting at their launch areas. He asked his senior meteorologist for his opinion. This officer reported late on the evening of 5 Jun that the General would have a window of four hours the following day in which to launch his operation. The General then committed Allied troops by saying: “Good, we go.” He didn’t ask to see the charts or wait until the next set of readings is available. He trusted his core staff and accepted the information given. Building that trust amongst the team is essential.

Clearly technology plays an increasingly important role in effective command and control. Information can be made available almost instantaneously. The risk is that we prevaricate and delay while waiting for the “golden” piece of information that will make any decision obvious. The data forming the basis of such information is contained within a myriad of different databases. There is little or no commonality of data structures. Attempts within the US and UK defence arenas to develop such data dictionaries have cost large amounts and singularly failed to deliver that which they promise. Every so often, we develop grandiose plans to field the definitive system that will replace all the legacy systems and do everything we need to bring about a common information backbone. So far, if these systems ever see the light of day, they are characterised by being over-budget,

late and never providing the promised levels of information management and availability.

The US Army has a highly complex logistics network. In the early 1990s, they developed a language named Standard Generalized Markup Language (SGML) to assist different logistic depots to identify key supplies, even when the individual units used different source codes. SGML has now been developed into the Extensible Markup Language (XML), the use of which permits hierarchy, extensibility and information enrichment. It requires much more memory than the traditional Relational Database Management Systems (RDBMS), but memory is now much cheaper than it was when such systems were initially developed. Tagging data, from whatever data source, allows search and comparison across any number of databases. No longer do we have to replace “legacy” systems with new and untried technology, but we can continue to allow their use and exploit the inherent extensibility of XML to make their data available across a wider audience. In support of the commander, XML tagging will allow the commander to focus upon that information he requires, rather than being subjected to the “fire hydrant” of information overload.

XML has been available for almost a decade and yet it has not made significant inroads into the more traditional RDBMS and Middleware solutions. In part, this is due to the inbuilt inertia of larger firms who have markets they wish to protect and prefer

to look at systems rather than at the data itself. There is also a perception that XML tagging “bloats” the data and slows down the search capability. Such “bloats” can be eliminated with algorithms designed to compress the data and allow for more rapid searching. In terms of data search, we are all now familiar with Google and the ease and speed of its data extraction to meet our stated requirements. Google provides a very broad response – how many times have we seen hits in excess of one million?

Information overload is as pernicious a problem as lack of information. Lt-Col John Boyd was a USAF pilot flying jets in the Korean War. The US was losing large numbers of aircraft and pilots, and Lt-Col Boyd recognised that the key problem was the excessive amount of information in the cockpit. When a surface-to-air missile was detected, all the aircraft alarms came on and pilots were distracted from the essential task of evasion. Lt-Col Boyd then developed his now famous OODA loop (Observation, Orientation, Decision and Action) to focus on operational and tactical priorities. He lived to be a highly successful retired Lieutenant Colonel! RDBMS, on the other hand, gives much greater specificity than Google, albeit with limited database connections if the speed of extraction is not to be excessive. The native XML tool can provide a fusion of both approaches, high-speed recovery with data specificity. XML, by its very nature, is extensible, which means that as search requirements change, new tags can easily be added to old data.

Overcoming the “Legacy System Problem”

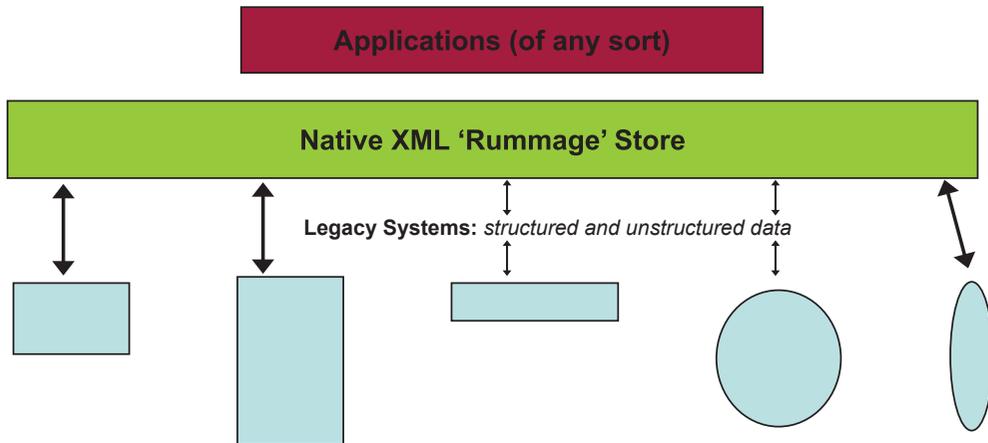


Figure 2. Overcoming the “Legacy System Problem”.

The success of such an approach, already proven in a number of systems, is that the legacy systems themselves can continue to be operational and used for the purposes for which they were designed. If, on the other hand, they are old and no longer of utility, the data contained, often application specific, can be stored as XML data on modern Windows or Linux platforms to be used as and when required, allowing the original system to be switched off.

In terms of the original NEC concept, this is a liberation of the data. For NEC to work, to be able to confront the decision maker with coherent information from a wide range of data sources in a manner in which he can assimilate it, and take timely and effective action, we need to focus on the data irrespective of the systems in which it might reside.

Let us briefly return to our submarine commander, deep in enemy waters. He represents the core difficulty of NEC in delivering IP to the soldier in the

foxhole. Use of a “virtual submarine” at the operational HQ allows command qualified watch-keepers to provide only those information considered to be relevant to, and focused upon, the submarine’s operational mission. In the diagram below, the information architecture allows for a “virtual operations centre” where all data streams directed towards that operational entity (ship, platoon, air-group, special forces, etc.) are received and ingested into an XML database. The original form of the data is preserved for audit and record.

Once ingested, the information content of messages, word documents, etc can be extracted and placed in the XML queue for sorting and prioritisation before onward transmission to the real operations centre in the field.

The issue of security of data, particularly in that “final mile” to the foxhole or submarine is critical and, while we endeavour to safeguard our systems, doing so in the operational environment can be more complex.

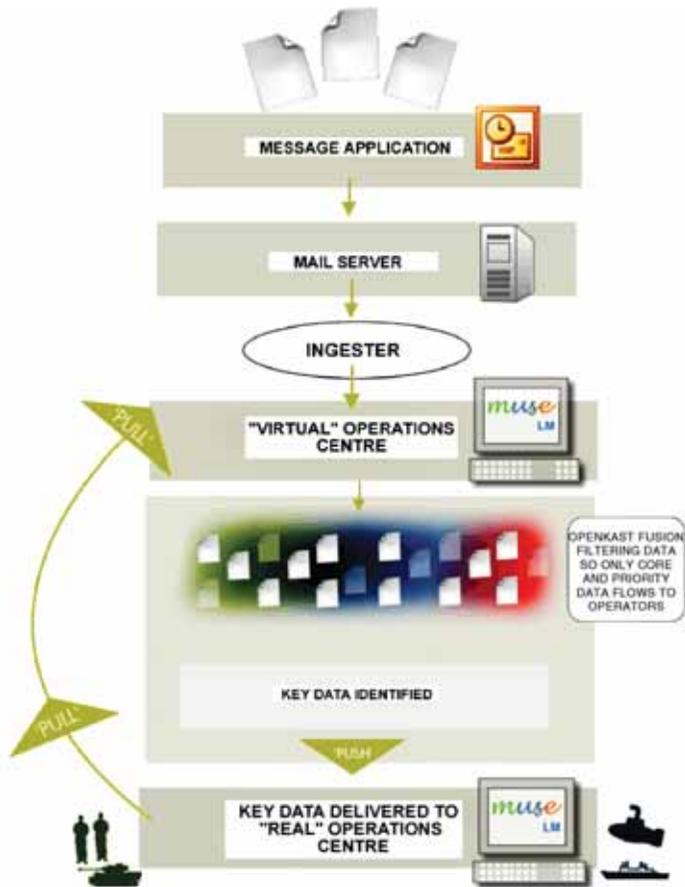


Figure 3. Use of a “Virtual HQ” to provide core information.

Conclusion

Network Enabled Capability is not a panacea for lack of investment in people. It will only work with the right people, acting as coherent and responsive teams, as well as employing the right technologies. The technologies supporting effective NEC are available today. Native XML search capabilities allow for the liberation of data from the confines of their respective databases. However, decision-making remains a core skill. Without such a skill, NEC is a wasted asset.

The ability to take effective decisions can be inculcated into junior officers and regularly put to the test throughout their careers. Fitness reports should balance an officer’s failures and successes to ensure that the entire corps learns from mistakes. Independence of thought is the principal ingredient of a successful general – eliminate it at your peril.

Data and information overload is the biggest deterrent to effective decision-making. Though technology can help, the bottom line is that decision-making

remains a command function. With the right doctrine and training put in place, and the right technology employed, I believe we are very much closer to making the NEC dream a reality. 

Endnotes

- ¹ Norman Dixon, *On the Psychology of Military Incompetence*, (Time Warner Books UK, 1991).
- ² Networked Enabled Capability: JSP 777 Ed1. Ministry of Defence, UK, 2005.
- ³ Speech to USAF IT Conference – reported in Federal Computer Weekly, August 2006.



Commodore(Ret) Patrick Tyrrell, OBE, is currently a Director of a small information integration company, TyrrellSmith Limited, and a Director of the Armed Forces Communications Electronics Agency (AFCEA). He joined the Royal Navy in 1976 and retired in 2002. While in service, he had served in submarines and the intelligence community. He was Commandant of the Defence Intelligence and Security School, and Deputy Chief Executive of the Defence Communication Services Agency. He has degrees in Chemistry (Oxford), Law (London) and Management (Portsmouth School of Management). He was awarded the Order of the British Empire by Her Majesty the Queen for his work on arms control in the North Atlantic Treaty Organisation.

Beyond the Velvet Curtain of Transformation – How the Future of Warfare will be Shaped

by CPT Gareth Wong



Even as the SAF embarks on the road map toward a 3rd Generation transformation, we need to begin evaluating the course of our development. In particular, beyond just focusing on current capability developments, we ought to be acutely aware of what is transcending elsewhere, in a constant quest to keep pace with the next phase of military

development. In an age of free-flowing information, no one country can afford to rest on its laurels and only seek to adapt from the experiments of others. Blazing a path forward from here requires us to be particularly discerning of global developments. It leads us to question: What lies beyond the 3rd Generation curtain? Is there any reason to look beyond this sphere?

Recent military conflicts serve as a useful reminder that it has become imperative to address how the ‘backdrop’ of warfare is altered when the enemy chooses not to play by the same rules. One would hardly expect any future adversary to simply amass conventional forces against a technologically superior military power. Indeed, what we now see is a metamorphosis of military tactics. When we consider that the likely battlefield of the future is one conducted in irregular urban/suburban close quarters where there is an intermingling of hostile, neutral and friendly parties, it is evident that the road ahead has been cut out not just for the SAF, but for any modern military. Juxtaposing these various considerations together, it is clear that a reliance on technological advancements alone is unlikely to prove efficacious. At the risk of sounding pedantic, this paper seeks to uncover some of the key challenges that the future military will face.

A Fourth Generation (4G) Paradigm

Not Like Yesterday...

Nearly two centuries ago, Carl von Clausewitz’s seminal work “On War”¹ established much of the modern way of state-war. From Waterloo to the two World Wars to Operation Iraqi Freedom, professional armies have been guided by the precepts laid out in his work. Clausewitzian theory proscribed that War was but merely “a continuation of policy by other means”², and that State and Regiment ultimately circumscribed war. However, one ought to question just how relevant such rules and demarcations are in addressing

the challenges of the future. Just as the Treaty of Westphalia in 1648 had marked the end of 30 years of religious wars and ushered in an era where the state possessed the monopoly over organized violence, events post-9/11 have marked the harbinger of a new era of non-state conflict already long-brewing on the sidelines. As Vietnam, Mogadishu, Bosnia, Rwanda and most recently Lebanon have demonstrated, the military has, more often than not, found itself coming out short because it was not the kind of combat they had expected to fight. Fought for a host of social-psychological purposes and desires, the conduct of combat by tribes, clans, and other traditional social units has proven to be vastly different.³

Former Commandant of the Marine Corps, General Charles Krulak, astutely admonished against a fixation on conventional thinking which he believed would only serve to confound future military operations. In an essay titled “Not Like Yesterday”⁴, he cited the example of Proconsul Quintilius Varus, who had led three powerful legions across the Germanic border to suppress tribal rebellion in AD 9; where only three years earlier he had decimated dissenters in a similar mission. His second exploit, however, proved to be a decisive failure for he had expected his adversary to fight *the Roman way*; yet “instead of coming out on to the plain where the legion could employ the shock power of its superior cavalry and lethal accuracy of its bowmen, these tribal warriors lured the Romans into marshes and forests, neutralizing Roman superiority”⁵. War does not remain stagnant, and just like Varus’s fixated outlook on warfare had

cost him dearly, modern militaries must similarly take heed or else suffer similar misfortunes.

What's Beyond a 3rd Generation?

In a 3rd Generation military paradigm, adversaries are still coined in terms of 'terrorists' and other identifiable groups. But is this conception likely to remain as relevant in the future? There exists a conundrum which a 'sense and strike', or a 'trigger to strike' networked system of systems is unable to fully address: when retaliation requires knowledge of who has launched an attack and the address at which they reside⁶, how well are conventional military capabilities geared to face this 'shadow-less' enemy⁷? Precision guided capabilities allow the military to accurately engage predefined visible targets, but the challenge in securing a total victory transcends beyond just being able to locate and destroy. Enemies in this era will certainly present fewer targets vulnerable to conventional attack, and their followers are more likely to be willing to fight and die for their causes. Wearing no uniforms and interspersed amongst the general population, these enemies present an imbroglio for both the offensive and the defensive.

In a prescient article published in the October 1989 issue of the Marine Corps Gazette, military historian William Lind believed that a new era of 'Fourth Generation Warfare' (4GW) would mark the future of warfare. In this age, the potential adversary any modern military is likely to face is an adaptive and resilient one; one that has "learnt to counter the conventional attrition doctrine of the

technology and firepower intensive forces of industrial based armies"⁸. And yet, academics believe that there remains a pervading "Dogma" in the military to win wars with 'successful conclusions'⁹. Operation Desert Storm in 1991 was a perfect embodiment of this: Clear aims and well-defined means, an asymmetrical and vastly inferior enemy; technological superiority and massed armies; and speedy maneuver coupled with fire-intensive operations.¹⁰ Operation Desert Storm was a textbook example of war-fighting, and in its aftermath, the US and other militaries planned for future wars with doctrine, training, and procurement all geared for this type of operation. In the 4G era, traditional strengths are now redefined – the focus is shifted away from technology to ideas. Conflicts shift from a matter of destroying military targets and regular conventional forces to social-economic or political-cultural 'centers'¹¹. In short, 4GW is not just another 'terrorism' or 'low-intensity conflict'; it is about how the weak (be it state or non-state) confront the military power of the strong.



Boy vs tank; 4GW is not just another 'terrorism' or 'low-intensity conflict', it is about how the weak confront the military power of the strong.

The advent of an age of 4GW thus places significant emphasis on asymmetric and complex irregular warfare; a future where war is “custom-designed” by hybrid adversaries that will avoid predictability or linear operations. Post-Cold War thinking that interstate warfare will *only* remain conventional in nature is fallacious; irregular warfare provides an aberration from anything that modern militaries have been accustomed to. The question is: What are some of the key success factors that modern militaries will need to deal with this new age of challenges?

Identifying a Center of Gravity – Is There More to It?

Carl von Clausewitz displayed remarked prescience when he asserted that war never remained a constant. Highlighting the notion of ‘friction’ in war, Clausewitz draws attention to the importance of recognizing the need to be fluid and dynamic in any military engagement. “Every war is rich in unique episodes. Each is an uncharted sea full of reefs. The commander may suspect the reef’s existence without ever having seen them; now he has to steer past them in the dark.”¹² War in the latter half of the 20th century emerged primarily along modern Western variations, but except for Desert Storm and the war-fighting phase of Operation Iraqi Freedom, this has not been the case since the end of the Cold War. Conflicts are now increasingly pitted between states and non-state armed groups¹³; be they tribal, ethnic, clan or religious.

It has been heavily asserted that modern militaries need to develop and maintain an ability to deal with a new

environment of terrorists, insurgents, militias and other criminal organizations. However, there is a greater requirement to develop an adaptive mindset to address any challenge, *regardless* of what form it may take. Beyond just developing a capability to address current problems, there is a need to maintain a capacity to pre-empt, stem and redress future problems. Clausewitz had once commented that, in combat, identifying an enemy’s center of gravity (COG) – “the hub of all power and movement on which everything depends”¹⁴ was key in dictating the success of any military campaign. This idea centers on the concentration of one’s power at the critical time and place for a decisive purpose, therein targeting the ‘weakest link’ to achieve success. Hitting out at an adversary’s center of gravity is clearly not a new idea. To address the challenges of an asymmetric future, however, requires an extension of this. It is now paramount to embark on a radical quest to defy convention to constantly identify new center(s) of gravity within a *creative adaptation/ application* of a new environment. Indeed, it is critical to consider that seemingly nebulous objectives (which can sometimes transcend physical realms) can also constitute plausible COGs.¹⁵

Information Warfare – The Next Stage

A Strategy or Tactic?

With the rapid development of technology and mass communication, much of the military’s development has centered on enhancing info-centric platforms, with particular emphasis on

the establishment of network-centric synergies to engage in a new era of ‘net-war’¹⁶. However, this idea still largely rests along tactical lines; one must then question: Can the next generation of warfare rest along lines manipulating information on a *strategic* level instead? The recent Israeli-Lebanon conflict gives an indication that this might very well be the case. For the Israeli Defence Force, the war represented a need to establish a line of security from which Hezbollah’s reprisal of Katyusha rockets could not target Israeli cities. For Hezbollah, the war represented a different campaign – a need to win a war of information. For the Israelis, information warfare remained a tactical tool in aid of a practical strategic objective; for Hezbollah, winning the information war itself was the ultimate strategic goal.

In his book “The Lexus and the Olive Tree”, Thomas Friedman coins the term ‘Super-Empowered Angry Man’ to describe the angry men that globalization creates.¹⁷ Termed ‘super-empowered’ because of globalization forces; anyone that hates globalization can now do something about it, more than ever, because of globalization. With rapid developments in technology, these groups can now take advantage of ‘cyberspace’ to overcome physical vulnerabilities; real-time war on the ground is now effectively intertwined with the electronic war. In a 4GW realm where pragmatic groups confront superior military power, information warfare will be engaged as a core competency rather than just a mere tactical tool. It is thus highly plausible that the emerging way of war will increasingly mean fighting *first* for information dominance. Conventional

wisdom on the interplaying roles of information *vis-à-vis* conventional operations will be radically challenged. The question remains: How should we approach information warfare? Is engagement at a tactical level appropriate? Will it be sufficient?

Perception Shaping – A New Frontier

Be it strategic or tactical, what can we identify as a plausible COG in an age of information warfare? In the last half of the 20th century, we saw a marked proliferation in the use of variegated forms of media that significantly chartered the courses of a number of conflicts. The 1968 Israeli El Al airline hijack by the Popular Front for the Liberation of Palestine (PFLP) was possibly the most significant milestone in the development of global terrorism; through a combination of “dramatic political statement, ‘symbolic’ targeting and crisis-induced de facto recognition”, the Palestinians and terrorist groups worldwide recognized how powerful manipulating public opinion could be.¹⁸ In recent times, Al Qaeda and Hamas have also relied heavily on the media to propagate terrorist activities and draw public support for their cause.¹⁹ Inherently, the engagement of information warfare involves an imperative dimension; that of *perception shaping*.

In Operation Iraqi Freedom, much emphasis was placed on the “utility” of precision-guided munitions, with Iraqi fortifications being targeted accurately with minimal collateral damage. Nonetheless, as Senior Producer from Al Jazeera, Hassan Ibrahim, puts it:

“Regardless of the number of civilians killed...it is no justification when a viewer sees that (the bombings)...See, the bombing of Dresden was *before* the days of television...Now when you see the massacres in Palestine... the idea is really infuriating...”²⁰ In this age, it is less about facts; it is about perception. It is about how people perceive things. The recent Israeli air strikes on Qana corroborate this fact exactly. During the strikes, a residential building housing refugees near Hezbollah rocket launching sites was destroyed in an act of collateral damage, stirring a worldwide outcry. Israeli arguments that this was part of Hezbollah’s strategy of endangering civilians intentionally to rouse anti-Israeli sentiment proved difficult to reconcile when moving images of the strikes’ gory aftermath were broadcast all across Arab news networks. Clearly, merely possessing sufficient intelligence as to an enemy’s whereabouts does not address the underlying difficulty in ascertaining the true *intent* of the adversary.

The recent Israeli-Lebanon conflict has indeed been a watershed in its own right: it has shown a possibility that being seen ‘too successful’ militarily may unwittingly lead to a backlash that undermines the overarching objective of eroding the influence of one’s adversary. For the first time in Arab-Israeli history, the question of who “won” remains very much an issue of contention. Perhaps, the issue of who ‘formally’ won is less important when we consider that Hezbollah was able to successfully mar any ‘decent’ form of victory that Israel was seeking to achieve. In this age, battling over conceptualizations of ‘victory’ has become an equally important tussle as achieving the physical victory itself. Indeed, ‘victory’ as we know it has become increasingly elusive. Thus, when we look at the psychosis of warfare, it becomes apparent that the issue of ‘perception-shaping’ is paramount in any form of combat that transcends, and it is likely that this will take on an increased profile in an era of 4GW.



The recent Israeli-Lebanon conflict in 2006; in this age, battling over conceptualization of ‘victory’ has become an equally important tussle as achieving the physical victory itself.

A Cultural Prologue in the Military

Considering the 4GW backdrop of future military campaigns, the cultural and anthropological foundations of traditional peoples and societies is another pertinent area that the modern military must seriously address. The study of culture, the “norms, values, institutions and modes of thinking in a given society that survive change and remain meaningful to successive generations”²¹, will help to shed light on the tactical, operational and strategic psyche of any group. To understand unconventional warfare, a new approach is thus needed – one that is anchored in historical, anthropological and traditional cultural narratives. The great Chinese military strategist Sun Tzu captured this idea perfectly: “...one who knows the enemy and knows himself will not be endangered in a hundred engagements. One who does not know the enemy but knows himself will sometimes be victorious, sometimes meet with defeat. One who knows neither the enemy nor himself will invariably be defeated in every engagement.”²²

The late Professor Adda Bozeman offered such an examination of world politics through the lenses of history, culture and anthropology.²³ In her 1976 work “War and the Clash of Ideas”, she discovered that conflicts and violence may well be accepted in most areas as part and parcel of everyday life. An understanding of why others fight can thus be derived by probing their mental and psycho-cultural roots of war, and other historical antecedents. Professor

Bozeman’s research leads us to question: if culture influences why ethnic, ethno-national, religious and communal groups fight, may it not also provide clues to understanding the influences on *how* they will fight? It is a question that has received little attention, but is a pertinent one that needs to be addressed.

Given the new spectrum of operations involving both conventional war-fighting and Operations Other Than War (OOTW), it comes as no surprise that the honing of Cultural Intelligence (CQ) has become one of the key competencies identified for the military. In particular, the need for cross-cultural leader competencies and awareness has been emphasized to allow for the development of cultural sensitivity to a variety of cultures.²⁴ Military leaders grounded in CQ abilities will be more effective in multinational operations, because of their ability to make “culturally sound” decisions. History has shown that a negligence of cultural awareness can lead to unwanted repercussions in the overpowering heat of combat. The Battle of Algiers, the My Lai massacres in Vietnam, and most recently the Abu Ghraib incident in Iraq; these are but a few examples reinforcing the resonant message that recognition of culture is ultimately still paramount.²⁵

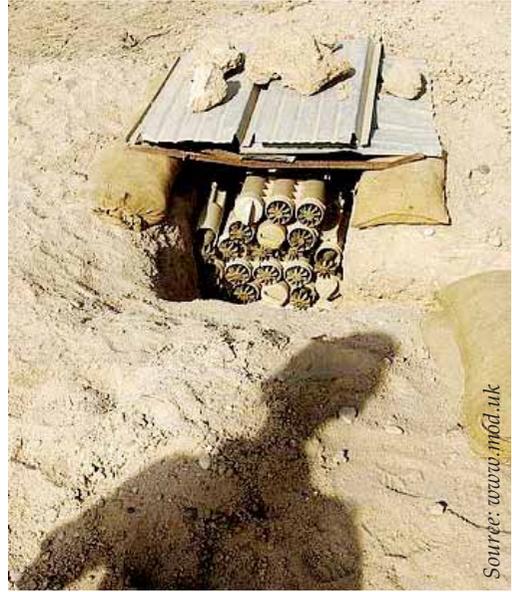
Undoubtedly, the challenge for both military and policymakers will be to recognize and analyze multiple distinct cultures as well as political systems that differ significantly in their modes of rational and normative thought. Singapore’s unique multi-religious/ethnic composition makes this an exceptionally important task in

light of this. It is thus imperative that we recognize this cultural COG, and begin engaging in historical, anthropological and cultural studies.

An Age of Resilience

Why Resilience?

MINDEF's mission statement has always been established on a need "...to enhance Singapore's peace and security through *deterrence and diplomacy*, and should these fail, to secure a swift and decisive victory over the aggressor".²⁶ Today, Singapore's renowned international stature stands as a testimony to the efficacy of this policy adopted since her independence. However, in a 4G era where rational states are sometimes no longer the primary actors, the lines become blurred, and conventional wisdom is radically challenged. Notions of 'strategic depth' become inconsequential when no nation can now depend on secure territorial borders to tackle an amorphous adversary. The fact that no attacks have been successfully carried out may not imply that a deterrence policy has been effective. Indeed, this is perhaps the *sine qua non* of a good deterrence policy: you can't *effectively see* effective deterrence.²⁷ In a 4GW scenario, reaction time becomes key, and deterrence must be complemented with reactance/consequence management. Indeed, responding to any unforeseen scenario may almost be as important as trying to deter one. To reach this proper synergy, an underlying foundation of population resilience is indispensable.



The 'shadow-less' adversary; in a 4G era where rational states are sometimes no longer the primary actors, the lines become blurred, and conventional wisdom is radically challenged.

This idea becomes even more significant when we consider the plausibility that 4GW will involve unconventional weapons in the overall strategy of 'terrorization'. The modern terrorist/insurgent no longer holds any moral disapprobation when it comes to the issue of inflicting casualties; the use of chemical, biological, radiological and nuclear (CBRN) weapons has become all the more significant. Indeed, the global community must be significantly aware that "it can no longer be assumed that the deliberate causing of mass civilian fatalities is impossible in the developed world"²⁸. The universality of a suicide bomber's possible target serves to foment an atmosphere of uncertainty and vulnerability amongst the general population, possessing a certain coercive

logic that “suggests that the attackers could not have been deterred by a threat of costly retaliation”²⁹. In this era, Brian Jenkins’ comment that ‘terrorists want a lot of people watching, but not a lot of people dead’ may significantly bear less truth.³⁰

As a case in point, the outbreak of the Severe Acute Respiratory Syndrome (SARS) epidemic in 2003 served to provide Singapore with many valuable lessons in tackling a biological threat, and also alluded to the need of beefing up population resilience. SARS impacted not just Singapore’s health system, but the entire economic and social fabric of the country. In responding to this unprecedented crisis, the government acted with immense alacrity, imposing stringent health controls and measures (such as quarantining anyone who had direct contact with infected patients); therein setting the example for the rest of Asia to emulate. It is heartening to note that SARS was eventually controlled not just via the efforts of the medical sector, but through the concerted works of all Singaporeans. This example again clearly exemplifies what is needed to counter any crisis-resilience; regardless of what form it might take.

What Resilience?

History has shown how powerful manipulating population resilience can be in combat. The case of Operation Barbarossa in World War II provides a lucid example. Despite suffering a series of initial defeats against a seemingly insurmountable German aggressor, the Russian people never acquiesced. Fighting an implacable, blood-thirsty German adversary only hardened the

Russian resolve to rise in a giant national effort to repel the invader. Defying German propagandists that they were “weak”, Russians rallied around Stalin’s call to rally around the flag, and this Soviet fighting spirit and will to fight was what proved to be indomitable.³¹ Operation Barbarossa evolved into an inextricable quagmire, wherein Russian resilience proved, much to German chagrin, the ‘silver bullet’ for which they had no reply to.

In building resilience, a quiet confidence in capabilities must first be established as a baseline. In a 4GW paradigm, although the premise for an effective strategy cannot rely on ‘waiting’ for attacks and then responding, there is a need for effective response measures to deal with attacks that are not effectively deterred. Here, achieving a “swift and decisive victory” may entail more than just a military rout over the adversary. The key is to ensure that national resources will be effectively channeled in times of national crisis³², with state organizations remaining functional. In totality, “an effective, integrated response requires incident management planning, enhanced interoperability and coordination, based on and supported by rapid and effective decision-making”³³. The employment of civil defense measures certainly by no means reduces the threats at hand, but it plays a critical role in ameliorating the resulting chaos.³⁴

Beyond the underlying hardware needed to rally confidence, the next step must focus on the ‘heartware’. Imbuing emotional strength is critical in determining the rapidity of the recovery and comeback process. Ultimately, when

terrorization is removed of its inherent ‘terror’, crises will be managed more effectively. The 9/11 attacks on the United States provides a useful illustration. The psychological impact of witnessing such an atrocity conducted on American soil certainly shook the American people. Yet, instead of languishing in its aftermath, the American people rallied together against the onslaught of global terrorism. The intrinsic challenge in building emotional strength lies in altering a population’s innate cognition to recognize a crisis from a pessimistic to an optimistic outlook.³⁵ Without the benefit of hindsight, or the advantage of clairvoyance, deterrence and resilience remain our best bet yet in targeting the ‘shadow-less’ adversary, and must be seen as an important defensive COG.

The End of the Beginning

Warfare in the future is likely to transcend mere conventional boundaries; indeed, it will be akin to a “Herculean” battle against a multi-headed Hydra.³⁶ The military will increasingly need to give due consideration to cultural and social paradigms that are likely to influence the future field of operations. Military operations, though paramount on their own, must be carefully calibrated according to political, social and economic imperatives. No matter how high-tech warfighting becomes, war is about the people and the military; it is thus not enough to dominate the technological domain alone.³⁷ It thus becomes evidently clear that beyond the immediate capabilities a military possesses, it is equally important to possess a tenacious lucidity in the policies that guide military affairs.

In conclusion, the notion of a 3rd Generation transformation has indeed aroused a frisson of enthusiasm across the board, but it is important that we do not lose this alacrity when it comes to thinking beyond a 3rd Generation status. The idea of a Technological Revolution in Military Affairs *per se* should not be taken as a *fait accompli*. Recent events perhaps mark the harbinger of a different face of war; part of which is unable to be addressed by a 3rd Generation capability alone. Indeed, the concept of a 4GW is not a chimerical one, and it remains to be seen just how effective modern militaries will be in rallying to address it. For the SAF, it is thus imperative that we instill not just a capability, but a capacity that will be able to withstand the test of time. 🇲🇲

(Ed note: This essay is the first prize winner of CDF Essay Competition 2006)

Endnotes

- 1 Carl von Clausewitz, *On War* (Penguin Books Ltd, Strand, London, 1968).
- 2 Michael Howard and Peter Paret, Carl von Clausewitz – *On War* (Princeton University Press, Princeton, New Jersey, 1976), p87.
- 3 Richard H. Shultz Jr and Andrea J. Dew, *Insurgents, Terrorists and Militias – The Warriors of Contemporary Combat* (Columbia University Press, New York, 2006), p6.
- 4 Foreword by General Charles Krulak to Richard H. Shultz Jr and Robert L. Pfaltzgraff, eds, *The Role of Naval Forces in 21st Century Operations* (Washington, DC: Brassey’s, 2000), ppxi-xii.
- 5 Shultz and Dew, *op. cit.*, p9.
- 6 Richard Betts, “The new threat of mass destruction”, *Foreign Affairs* Vol.77 Issue1 (Feb 1998), p28.
- 7 Retired US Marine Corps General Anthony Zinni sums this up aptly: “The military does a damn good job of killing people and breaking things...And we’re so far ahead of any potential enemy right now in those kinds of technological areas...and all the things that make military units great on the battlefield, that you wonder why we keep busting brain cells wondering how to

- continually do it better, or to transform it into something else...But that is not the problem, and it hasn't been...what we have to ask ourselves now is, is there something that the military needs to change into that involves its movement into this area of the political, the economic, the information management?" – General Anthony Zinni, Address to the Naval Institute Forum, 4 Sep 2003, Gateway Marriott, Arlington VA, <http://www.mca-usniforum2003.org/forum03zinni.htm>
- ⁸ Chuck Spinney – "Ready for What?", <http://www.d-n-i.net/fcs/comments/c189.htm>
- ⁹ Andrew F. Krepinevich Jr., *The Army and Vietnam* (John Hopkins University Press, 1986), pp4-5.
- ¹⁰ Andrew F. Krepinevich Jr., *The Army and Vietnam* (John Hopkins University Press, 1986), pp4-5.
- ¹¹ Shultz and Dew, *op. cit.*, p20.
- ¹² G.I. Wilson, John Sullivan and Hal Kempfer – "4GW: *Tactics of the Weak confound the strong*", http://www.military.com/NewContent?file=Wilson_090903 (8 Sep 2003), p3;
- Special Dispatch – Jihad and Terrorism Studies: The Middle East Media Research Institute (MEMRI), February 10, 2002 No. 344: "Fourth-generation warfare...is a new type of war in which fighting will be mostly scattered. The battle will not be limited to destroying military targets and regular forces, but will include societies, and will [seek to] destroy popular support for the fighters within the enemy's society. In these wars...television news may become a more powerful operational weapon than armored divisions...the distinction between war and peace will be blurred to the vanishing point..."
- ¹³ Howard and Paret, *op. cit.*, p120.
- ¹⁴ Defined as "groups that challenge the authority of states, use violence in unconventional, asymmetrical and indiscriminate operations to achieve their aims within and across state boundaries"; Shultz and Dew, *op. cit.*, p13.
- ¹⁵ Harry G Summers, *On Strategy: a critical analysis of the Vietnam War* (Random House Publishing Group, New York, 1995), pp128-129.
- ¹⁶ In Singapore's case, our image as a safe and intensely protected country proves to be one such COG. The planned attacks by Jemaah Islamiyah in December 2001 underscore this idea clearly. The attacks should not be considered as an irrational one-off terrorist attack, but taken in concert with the increased streamlined-targeting exemplified by terrorist groups across the board. The attacks, if successful, would have been paralyzing for Singapore, and was clearly conceived as a nerve point by the terrorists.
- ¹⁷ John Arquilla & David Ronfeldt, *Networks and networks: the future of terror, crime, and militancy* (RAND, Santa Monica, California, 2001), p6.
- ¹⁷ Thomas L. Friedman, *The Lexus and the Olive Tree* (First Anchor Books Edition 1999), p398.
- ¹⁸ Bruce Hoffman, *Inside Terrorism* (Columbia University Press, 1988), p70: For the Palestinians, they certainly recognized how the manipulation of the media had advanced their cause "much more effectively than 20 years of pleading at the United Nations" had been.
- ¹⁹ Media clips exalting the terrorists in all their immaculate glory, before and after the terrorist act, are now commonly broadcasted in real-time in the Middle East. A notable example was Abu Musab Zarqawi's beheading of journalist Nicholas Berg in May 2004, which sparked an outcry on the use of such televised propaganda spurning the West.
- ²⁰ Extracted from the documentary 'Control Room' (Magnolia Pictures, 2004, Noujaim Films Production).
- ²¹ Shultz and Dew, *op. cit.*, p27.
- ²² Ralph D. Sawyer, *Sun Tzu – Art of War* (Westview Press, Colorado, 1994), p179.
- ²³ See Adda Bozeman, *Politics and Culture in International History* (Princeton University Press, Princeton, 1960), pp5-6: As a firm advocate of the utmost importance of culture, Professor Bozeman frequently contested the universality of American or European ideals and institutions. One of her contributions involved championing a theory that native modes of thought and behavior were never subjugated to Western Culture, and only remained dormant until a time it could re-surface; "Indigenous patterns of life and thought became blurred during the centuries of European supremacy ... It was not permanent because the Occidental world order was not easily compatible with the traditional local orders. As European domination retreated...they returned to their own pasts... to resurrect their realities and myths...to reinstate their native modes of thought and behavior."
- ²⁴ See Kok Yee, Ng, Ramaya Regena, Teo Tony M.S and Siok Fun, Wong, "Cultural Intelligence: Its Potential for Military Leadership Development", Presented at the 47th International Military Testing Association, Singapore, 8-10 Nov 2005, where Cultural Competence can be defined as "a set of cultural behaviors and attitudes integrated into the practice methods of a system, agency or its professionals that enables them to work effectively in cross-cultural situations".
- ²⁵ Zinni, *op. cit.*: "These are now culture wars that we're involved in. We don't understand that culture...We don't understand what makes them tick. We don't understand where we are in our own history. We don't understand what our role is in moving this away from a disaster for the entire world, and for us and our interests."
- ²⁶ http://www.mindef.gov.sg/imindef/about_us/mission.html

- ²⁷ Robert Trager and Dessie Zagorcheva, "Deterring terrorism: It can be done", *International Security* Vol.30 No3 (Winter 2005/2006), pp87-123.
- ²⁸ Fraser & Dando, *Genomics & future biological weapons* (Nature Publishing Group, 2001), p253.
- ²⁹ Robert Pape, "The Strategic Logic of Suicide Terrorism", *American Political Science Review* (Aug 2003), p347.
- ³⁰ Karl-Heinz Kamp, Joseph Pilat, Jessica Stern & Richard Falkenrath, "WMD Terrorism: An exchange", *Survival* Vol.40, Issue4 (Winter 1998/1999), pp168-183.
- ³¹ Mike Ruzza – "The Failure of Operation Barbarossa", *Military History Online* <http://www.militaryhistoryonline.com/wwii/articles/failureofbarbarossa.aspx>
- ³² This is applicable to the case for WMDS as well; within the SAF, active measures have been taken to reinforce national defences against biological and chemical attacks, with improved training for civil defence personnel in handling bio-chemical attacks: A number of notable exercises have since been conducted, such as Exercise Diamond Shield involving units of both the SAF CBRE Defence Group working in tandem with civil defence personnel to counter an Improvised Explosive Device (IED) and a chemical device. In 2005, emergency response personnel from Singapore and Johor engaged in a joint exercise involving spilled 'hydrochloric acid' at the Second Link in Tuas. It was the fifth such dry run held by the National Environment Agency (NEA) and Johor's Department of Environment since 2000 to test operational capabilities and foster better chemistry between the two sides.
- ³³ *US National Strategy for Combating Terrorism* (February 2003), p27, http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism/counter_terrorism_strategy.pdf
- ³⁴ As Richard Betts sagaciously admonitions: "Such programs would not make absorbing attacks tolerable. But inadequacy is no excuse for neglecting actions that could reduce death and suffering, even if the difference in casualties is small": Betts, *op. cit.*, p31.
- ³⁵ In Singapore's case, one would plausibly question how resilience would be instilled without strategic depth. This would certainly require Singapore to possess the ability to sustain strikes that may plausibly cripple existing infrastructure at hand. Certainly, an interesting extension would then revolve around considering if that would work to Singapore's advantage/disadvantage in the face of any perceivable attack. Perhaps, in times of absolute critical despair, resilience will become a natural call to order.
- ³⁶ Scott Atran – "A Leaner, Meaner Jihad", *New York Times*, Mar 2004, p2.
- ³⁷ Wilson, Sullivan and Kempfer, *op. cit.*, p5.



CPT Gareth Wong is currently a Platoon Commander in 4 SIR. An Infantry Officer by training, CPT Wong is a SAF Overseas Scholar, and he holds a Bachelor of Science (First Class Honours) in Economics from University College London, U.K., and a Master of Arts in Political Science from Columbia University, USA.

Diffusing the Fog of War – Superior Decision-Making in a Networked Environment

by MAJ Liew Hin Ban



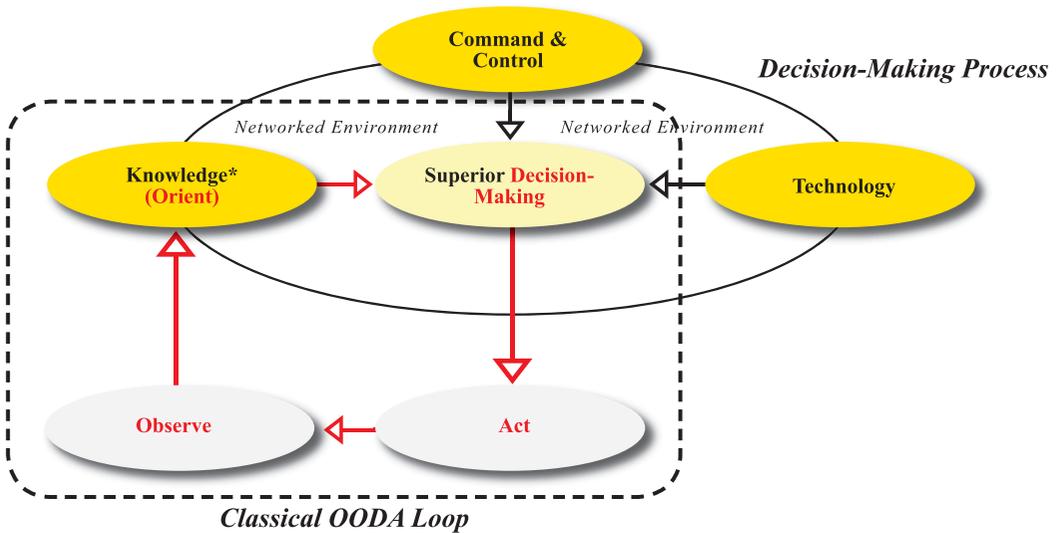
INTRODUCTION

“Therefore, the force of those skilled in warfare is overwhelming, and their timing precise....Even in the midst of the turbulence of battle, the fighting seemingly chaotic, they are not confused.”

- Sun Tzu

Network Centric Warfare (NCW) relies on distributed sensor elements, computer-processing power and networked communications technology to provide a shared awareness of the modern battle space. Shared awareness,

stemming from information superiority, increases synergy for command and control, and ostensibly resulting in superior decision-making.¹ But what constitutes as superior decision-making in a networked environment? What should the SAF do, in terms of technology, cognitive and command/leadership aspects, to realize and optimize the decision-making superiority, given the information advantage afforded by Integrated Knowledge-based Command and Control (IKC2), whilst circumventing the pitfalls? As the SAF strides forth



*By “orient”, John Boyd meant analysis and synthesis based on new information, previous experience, cultural tradition, and genetic heritage, to shape “the way we interact with the environment – hence orientation shapes the way we observe, the way we decide, the way we act”. This is synonymous with knowledge.

Figure 1. Integration of Decision-Making Process into the OODA Loop.

into a networked battlespace with IKC2, enabled by technology so that real-time information can be shared amongst units, we must remain cognizant of the fact that being endowed with technology and information are not a presupposition to superior decision-making.

Decision-making in a networked environment should be viewed as a systemic process in itself, involving the key aspects of *Technology*, *Command & Control* and *Knowledge*. Superior decision-making, as a concept, is borne out of the balanced consideration of these three aspects. It is arguably the crux of NCW – the ability to integrate information, anticipate, plan and ultimately decide. The relational model, as shown in Figure 1, contextualizes the classical OODA loop into the networked environment for purpose of accentuating the importance of *KNOWLEDGE*, as well as *Command & Control*, that perhaps

may have been overly shrouded by *Technology*, in relation to the decision-making process.

This paper argues for a holistic approach to decision-making in a networked environment that encompasses the aspects of *Knowledge* and *Command & Control*, in addition to *Technology* as a complementary enabler. While this paper is not *the all* on how to achieve decision-making superiority in the networked environment, it aims to take a systemic view, broaden awareness, offer preliminary advice or considerations, and indicate areas where emphasis should be placed. Ultimately, it is hoped that the research findings would provide insights for due consideration in the further advancing of the SAF’s IKC2 initiative, that may otherwise have been obviously dismissed due to interdisciplinary partitions.

TECHNOLOGY

“The most exciting breakthroughs of the 21st century will not occur because of technology but because of an expanding concept of what it means to be human.”

- John Nasbitt

The dawn of the information age has revolutionized the way the military organize, train, and fight. Advanced information technology offers the opportunity to improve the ability to achieve information superiority to reduce the fog and friction of warfare. But as networked warfighters execute critical real-time decisions that shape the outcome of battles, “the certainty of information conspires to slow and confuse that process”.² The advent of network-centric warfare will introduce new layers of human decision-making complexity never before experienced in command and control.³ Warfighters will need command and control decision support that facilitate the rapid assessment, planning, and execution of missions, often in the face of complex and uncertain situations. Decision-Support Systems (DSS) afford us such a support in organizing, exploring, and recommend options across a spectrum of military operations.

‘Satisficing’ DSS

In recent years, the design considerations and methods of analyzing decision-making, in the context of DSS, have evolved quite significantly, catalyzed by the dynamic operating environment of both the business and military realms. The classical approaches,

ranging from systems analysis to cost-benefit analysis, that focus on optimizing choices for a given idealized situation have been increasingly supplanted by developments that focus on the need to “understand the target systems, to confront ubiquitous uncertainty, and to identify strategies that are flexible, adaptive, and robust rather than optimal for some point case”.⁴

The design paradigm for a military DSS should be one that does not focus on deriving optimal solutions, as it is evident that in a command and control context, “it is not possible to include every single variable or combinations of variables that could impact a final solution”.⁵ The concept of “satisficing” is an interesting one that bears great insights for the design of the DSS in the networked battlespace. “Satisficing”, a term coined by Herbert Simon, is a hybrid term that attempts to express the combined essence of both satisfying and sufficing. It refers to the fact that when human beings are presented with numerous choices, we usually select the first reasonable option, rather than the best one available.⁶ Though, arguably, this notion is a realist’s perspective of how decisions are taken, it would resonate well with the psyche of the warfighter especially in time-critical situations that may significantly impact mission outcomes or lives. In the context of the battlefield, deciding on a solution that is good enough, robust, and quickly reached would be more tenable as opposed to one that involves complex and time consuming computation, which may not be accurate in the first place due to incorrect assumptions.⁷

Planning under Uncertainty

A key DSS development that accentuates this vein relates to planning under uncertainty. As alluded, instead of focusing on predicting effects and optimizing choices, based on a particular set of surmised assumptions, planning under uncertainty emphasizes exploratory analysis to assess the range of conditions under which a given strategy would give good enough results, as well as the range of conditions under which the strategy would fail. In essence, the paradigm of exploratory analysis is to develop “flexible, adaptive, and robust strategies that are relatively less sensitive to problems such as being surprised by an enemy tactic”.⁸ This approach is based on the concept of Complex Adaptive Systems (CAS) to help model a complex system or environment fraught with non-linearities and sensitivities. Interestingly, proponents of CAS have argued that Effects-Based Operations (EBO) need to be addressed within the CAS paradigm.⁹ Given that CAS would better characterize the qualitative nature of EBO, it would place users of CAS-based-DSS in good stead in planning and waging a “war of effects”.

KNOWLEDGE

“Machines don’t fight wars. People do, and they use their minds.”

- John R. Boyd

Technology, despite all its prowess in waging war, offers but a transient advantage. History has consistently shown that those who have mastered the use of new technologies were only able to hold a temporal strategic advantage over adversaries who were slightly

straggling behind. Arguably, warfare in the 21st century will continue to see such a trend. While the new source of power comes from information that is undergirded by the network, this power will not be exclusive, as information-network technologies tend to be inclusive. Adversaries will exploit the network to their fullest advantage and Al Qaeda for one has well demonstrated such abilities. However, such power has value only when the information has been used to create knowledge to aid in decision-making situations.

The new warfare thus highlights the rising importance of having a knowledge advantage over adversaries. It is posited that the comparative advantage of the network will no longer reside in the physical realm; rather it is the cognitive aspects, at the individual, group and organizational levels, that would demand emphasis in the networked environment.

Power to the People...Cognitively

The fog and friction of war will continue to loom over the networked battlefield. It does not discriminate by cause or physical capabilities. As adversaries exploit networks, new leverage must be sought to improve the warfighters’ ability to use information in thinking above the fog as the comparative advantage. The new warfare will demand unprecedented levels of initiative, decision speed, adaptability and collaboration. It will then “require that more of our people do new and much more complicated cognitive tasks more rapidly and for longer continuous periods than ever before”.¹⁰



The new warfare will require our people to do new and more complicated cognitive tasks more rapidly and for longer continuous periods.

The essence to achieving comparative cognitive advantage lies in improving how people sense, reason, decide, and act under pressure and in the face of complexity. As with the business realm, warfighters in the new era need to be imbued with strong intuitive and reasoning skills, a predisposition toward learning, and a willingness to take responsibility and risk failure.¹¹ This will place them in good stead to deal with the current and future operational environments that call for the integration of reasoning and intuition. Lachow et al calls such a quality as “battle-wisdom”.¹² Accordingly, a “battle-wise” soldier relies on intuition when decisions must be made quickly and under great duress against the backdrop of a dynamic and volatile environment. By relying on experience and seeking a “satisficing” solution, such a warfighter

can quickly deduce an appropriate course of action that is suited for that particular context.

Nurturing Battle-Wisdom in the New Age

In building a battle-wise military, Lachow et al posits a three-fold strategy¹³:

1. Improving the cognitive abilities of warfighters at the individual level.

The first fold relates to the comprehensive development of battle-wise individuals. It essentially calls for a re-examination of the process of selection and education of warfighters to solve problems in combat that is increasingly characterized by unfamiliar circumstances and inundation of information. Warfare in the networked environment would demand attributes that support decision-making, namely, anticipation, decision speed, opportunism, rapid adaptation, willingness to take personal responsibility, and the capacity for self-directed learning.

Another aspect relating to education and training that is seldom emphasized in a formal and conscious manner is intuition. Intuitive-based decision-making would possibly provide the added avenue to improve the ability of warfighters to make quick, accurate, and reliable decisions in complex, dynamic and ambiguous situations. Accordingly, one way to improve the intuitive aspect of decision-making is to isolate the types of decisions needed in a range of contingencies. The objective is to allow trainees to practice those decisions repeatedly, review the consequences, and make appropriate

adjustments next time around.¹⁴ This approach has been realized in the U.S. Joint Fire and Effects Trainer System (JFETS)¹⁵ that focuses on the development of the soldiers' cognitive skills and decision-making ability in high-pressure, time-sensitive environments. To this end, warfighters must be able to move between formal reasoning and intuitive decision-making quickly and seamlessly. This is the basis of the notion of "battle-wisdom" that may be a decisive factor in determining the outcome of future conflicts, and it starts with the individual.

2. Enhancing the collective cognitive power of teams.

The second fold moves into the collective order of teams wherein collective intelligence is derived from teams to tackle particular operational problems. Based on network theory¹⁶, this ostensibly delivers sounder decisions and offers greater flexibility than vertical command and control. Though promising in theory, achieving "battle-wisdom" at the team level will be difficult. The authors recognize that there is a time-information trade-off between the cognitive speed, agility, surprise, and adaptability derived from singular decision-making and the quality of decisions based on the informed views of the team members. Ultimately, it is purely situational as to which mode of decision-making is best suited. Guided by the same principles of improving the cognitive abilities of the individual warfighter but at a macro level, the authors suggest that a reasonable starting point would include: a provisional decision-making approach to gain time and information, self-awareness of collective experiential and analytical limits, the ability to learn in action, and an emphasis on the abilities

that create operational time-information advantages, namely, anticipation, rapid decision-making, opportunism, and quick adaptation amidst a dynamic environment. While it would seem that harnessing of individual cognitive powers into a collective form would face practical challenges, it must be recognized that there exists the latent form of collective wisdom that must not be dismissed but actively pursued in a concerted manner despite it requiring further thought, research and experimentation.

3. Reforming command and control to harness these abilities.

The final fold provides the overarching mechanism that will bring to bear the true power of distributed cognition. This calls for decentralizing decision-making authority, making it necessary to re-examine the command-and-control architectures that will facilitate the shifting of authority downward and outward. It expands the opportunity for more effective cross-boundary collaboration, and enabling warfighters, units and whole forces to exercise "battle-wisdom" at the lowest appropriate level. This key aspect will be discussed in detail in the next section on Command & Control.

Command & Control

"Leadership is more tribal than scientific, more a weaving of relationships than an amassing of information."

- Max DePree

As modern battles are being commanded and controlled in the digital realm, the strive to deal with friction

and uncertainty, despite being enabled by technology, becomes paradoxical. What must then prevail are the human aspects that rein in the raw prowess of technology rather than be driven by it, in particular, the need for resolved military judgment in arriving at sound, reasoned and expedient decisions, despite the inundation of information and increased ops tempo. In this regard, this section discusses how network-centric operations may affect or impact the development and sustainment of military judgment and leadership, in essence, battlefield command. The Competency-Authority-Responsibility (CAR) model will be featured to help draw out the issues in a systematic manner, and consequently, frame the desired organization structure, culture and leadership qualities needed to augment decision-making in the networked environment.

Command Model – CAR

Paradoxically, “in spite of advances in technology, command will always be limited by human attributes and capabilities, and will rely on a commander’s creativity and intuition”.¹⁷ Command is thus a uniquely human characteristic where “all individuals can creatively express their will to accomplish a mission”.¹⁸ In characterizing the ubiquitous and innate capability of command within us, McCann and Pigeau posits that the three dimensions of Competency, Authority and Responsibility (CAR) “form an abstract three-dimensional space within which the Command potential of all military personnel lie”.¹⁹ They explain, “...there exists a

roughly linear relationship among the three dimensions, one that reflects an optimal balance for different levels of Command”. Such a balance exist in the Balanced Command Envelope (BCE) wherein dangerous or ineffectual command are kept at bay, while at the same time ensuring that motivation and initiative are maximized.²⁰ While it is envisaged that every individual’s command potential lie within the BCE, imbalances will naturally occur due to misalignment amongst the command dimensions of Competency, Authority and Responsibility. Invariably, the networked environment stimulates the relational changes amongst these associative dimensions.



Command in the Information Age calls for greater empowerment to individuals at the edge of an organization that will afford adaptability and agility to dynamically respond to increased uncertainty, volatility and complexity.

New Order of Decision-Making – *Multiplicity, Simultaneity, Responsiveness*

Applied in the context of the network-centric war environment, the CAR model surfaces some poignant observations in relation to decision-making by commanders. In essence, it alludes that as power shifts from the center to the edge, commanders must change the way they think about information and its dissemination, and about organizing and accomplishing tasks. Command in the Information Age is ultimately not the sole responsibility of any single individual. The function of command will be accomplished in a distributed and collaborative fashion, with shared and distributed responsibility. No single commander can control the detailed actions of such a large number of people and agencies.²¹ This calls for greater empowerment to individuals at the edge of an organization that will afford adaptability and agility to dynamically respond to increased uncertainty, volatility and complexity associated with military operations of the future, not just current times. This is the essence of the concept called Power to the Edge.²² According to Alberts and Hayes, the added dimension of organizational power is unleashed by moving power to the edge, where the organization interacts with its operating environment to have an impact on that environment with greater preponderance. Amongst others, an edge organization will be recognized by its key trademark characteristics of widened social networks enabled through appropriate interactions and inherent agility to deal with uncertainty and unfamiliarity as knowledge, experience and expertise

can be brought to bear responsively. In relation to decision-making, it is principally “everyone’s job”.²³ With greater access to information, knowledgeable individuals within the organization can and will want to be the decision-makers – if they are empowered to do so. Leaders must then be willing to divest their power and authority that will enable “edge members” to conduct their own decentralized decision-making and action within the context of the command intent. Because multiple decisions can occur simultaneously, the tempo of operations can increase exponentially.

We need to realize that as organizations are now compelled to draw upon a wider range of knowledge sources and points of view in order to comprehend the complex and unpredictable forces shaping the environment, there is a need to accentuate the new order of decision-making, namely, *multiplicity, simultaneity, responsiveness*. Superior decision-making in a networked environment must account for these new order attributes and not just focus on arriving at better decisions. McKenzie and Winkelen offers two insights in reinforcing this notion, namely, paying attention to the diversity of information and knowledge that we use for decision-making, and paying attention to aligning decisions.²⁴

However, distributing authority is not enough. Increasing the performance of an organization, as a whole requires a suite of attributes, which includes, the combined and individual cognitive strengths of warfighters, their readiness to take responsibility, and their adeptness at acting in concert.²⁵ The

next section will put the framework of *Technology, Knowledge and, Command & Control* in context for the SAF in deriving operational strategies and considerations for the furtherance of its IKC2 initiative in relation to decision-making.

CONCEPT OF SUPERIOR DECISION-MAKING FOR SAF IKC2

“Chance favors only the prepared mind.”

- Louis Pasteur

The motivation for this research stems from the notion that decision-making in a networked environment should be viewed as a systemic process that involves the key aspects of *Technology, Knowledge and Command & Control*. It posits that superior decision-making, as a *concept*, is borne out of the balanced consideration of these three aspects. The *concept of superior decision-making*, arguably an abstraction, serves to frame and concert the constitutional elements in a coherent manner to place the SAF in good stead in realizing and optimizing the decision-making superiority afforded by the networked environment. In this regard, a conceptual framework has been proposed.

The conceptual framework should not be misconstrued as a prescription that delves into specifics or speculative programs. Rather, it should be viewed as a cornerstone in guiding operational strategies for developing and realizing decision-making superiority in a networked environment, whose

potential would have otherwise been obviously suppressed by interdisciplinary partitions. Efforts in these three domains must go hand-in-hand. Although such efforts will involve sundry initiatives in disparate areas, it is important to pursue them within a purposeful and coherent strategy guided by a framework.

Another key purpose of such a conceptual framework is that it facilitates a common understanding of what decision-making superiority is all about at all levels – from the strategic leadership to the strategic corporal. As alluded in the discourse on command and control, power will increasingly be divested to the edge of the organization and we must not presuppose that superior decision-making is an inherent product of such a ‘phenomena’ with an equal understanding of it. We need to translate tacit understanding of what superior decision-making into a formal dimension within which thinking soldiers of the SAF are able to understand, internalize and exercise.

Conceptual Framework

The proposed conceptual framework for superior decision-making in a networked environment is pictorially represented in Figure 2. It maps the salient points from the balanced consideration of the three key aspects into a coherent ensemble for navigation through the networked realm. The research findings suggest that nine key attributes should be nominally accounted in the quest for decision-making superiority.

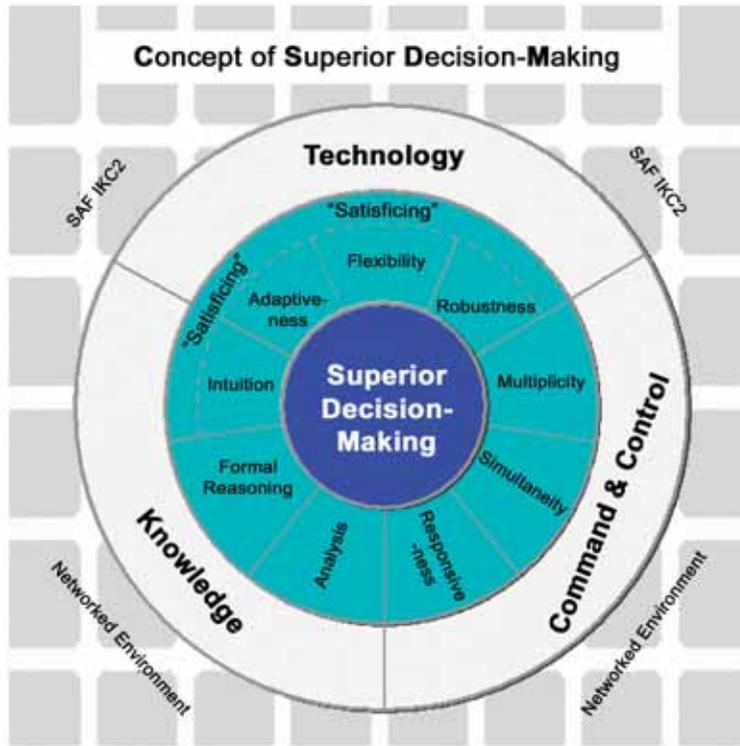
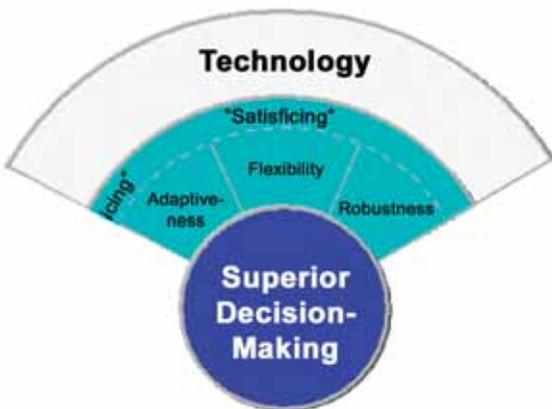


Figure 2. Proposed Conceptual Framework for Superior Decision-Making.

While this is by no means fully exhaustive, it serves as a baseline reference to facilitate a conscious, conscientious and concerted endeavor, instead of an incidental or fragmented approach towards such a quest. We shall next discuss this framework in context of the SAF to draw out broad areas of emphasis, as well as indicate where research and analysis may be needed.

Technology: Adaptive, Flexible and Robust... Yet “Satisficing”

Warfare in the networked realm will introduce new layers of human decision-making complexity never before experienced in command and control. Given the urgency, time pressures and inundation of information, SAF warfighters will need command and control decision support that facilitate the rapid assessment, planning, and execution of missions, else the cognitive limits of the warfighter may limit the success of network centric operations. Recent DSS developments have been focusing on the key theme of uncertainty. There has been a significant shift from “predicting and optimizing” to a strategy that imbues *flexibility*, *adaptiveness*, and *robustness*, which is more suited for

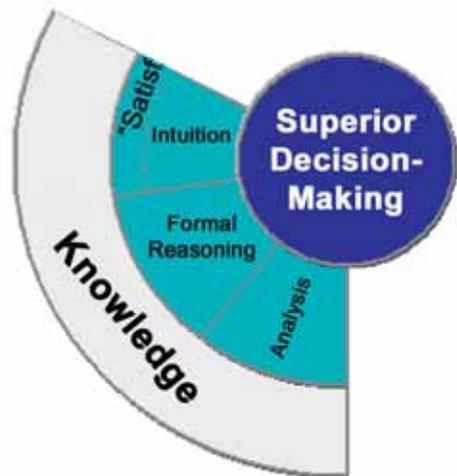


the complex and dynamic battlefield. The SAF's design paradigm for DSS should be in consonance with this philosophy. The concept of "satisficing" should be melded with this paradigm to accentuate flexibility and adaptiveness. A latent advantage of "satisficing" that should be invoked is its "less-rational" principle, which makes prediction difficult or unreliable for the adversary. This advantage was played out in real life, when Deep Blue defeated Garry Kasparov in a chess game by adopting a "satisficing" position; it was "playing like a human".²⁶ This creates an avenue for achieving comparative cognitive advantage that the SAF should exploit maximally.

The SAF should also take note that the ubiquity of the network and the effects-based paradigm will drive the next wave of military DSS development. The advent of network-centric warfare, juxtaposed against EBO, will fundamentally change one's concept of the "larger system" in the way it works. This impacts the analysis process of DSS in the aspects of conceptualization of issues, the creation of alternatives, and consequently, its analysis. While it is unclear what new generation of models and simulations are needed in military analysis and decision support to fully account and exploit the prowess of the network and EBO, it is evident that the future of decision-support systems will no longer be based on prediction and optimization.²⁷ Rather, the new paradigm of *flexibility*, *adaptiveness* and *robustness* will be of fundamental importance to the future of decision-support systems. The SAF must move with this "new order".

Knowledge: *Between Reasoning & Intuition for Cognitive Advantage*

The old adage of "Knowledge is Power" finds new meaning and vigor in the networked battlefield wherein a decisive outcome is predicated on having a knowledge advantage over the adversary. However, such power has value only when the information has been used to create knowledge to aid in decision-making situations. This comparative advantage is gained by leveraging on the cognitive aspects, at both the individual and collective levels. Specific cognitive abilities that are deemed crucial for operational success include, anticipation, reaction speed, opportunism and adaption.²⁸ These must be directed towards accomplishing the commander's intent (*Auftragstaktik*²⁹ – arguably a method of leadership), which demands high levels of cognitive integration. These are key attributes that the SAF should seek to nurture and develop within warfighters. It must not be presupposed that being plugged into the information rich network would endow warfighters with cognitive abilities, nor that they will be able to



exercise such abilities at will without proper and concerted education and training. On the same note of education and training, the SAF needs to ensure that its military education system places more emphasis on analysis, as opposed to facts, given the challenge in dealing with information overflow whilst adapting and responding to the dynamic environment.

Warfighters in the new era need to be imbued with strong intuitive and reasoning skills to deal with the operational environments that call for the integration of these two qualities, as well as the ability to seamlessly switch between them as the situation demands. The notion of “battle-wisdom” by Lachow et al is an interesting one that deserves to be further examined for possible adaptation by the SAF in its quest to gain cognitive edge over the adversary. Accordingly, a “battle-wise” soldier relies on intuition when decisions must be made quickly and under great duress against a complex and dynamic backdrop. By relying on experience and seeking a “satisficing” solution, the warfighter can responsively deduce an appropriate course of action. This is in consonance with the proposition for decision-support systems to adopt a “satisficing” logic in view of time-criticality and uncertainty.

**Command & Control:
*Power to the People in
Multiplicity, Simultaneity and
Responsiveness***

Command in the networked era will not be the sole responsibility of any single individual; it will be



accomplished in a distributed yet collaborative manner, characterized by shared responsibility. This calls for greater empowerment to individuals at the edge of an organization to afford adaptability and agility in responding to the complex and volatile environment. As power shifts to the edge, commanders must change the way they think about information and its dissemination, and about organizing and accomplishing tasks. The SAF needs to embrace this new yet inevitable shift of power and align its command and control processes to maximally harness its potential in unleashing a new order of decision-making prowess that is characterized by *Multiplicity*, *Simultaneity* and *Responsiveness*. Superior decision-making in a networked environment must account for these new order attributes and not just focus on arriving at better decisions.

The SAF, however, must be cautious in not presupposing that networked warfighters will be able to make reliable decisions by virtue of their empowered status or having been equipped to do so. The outcome of any operations will

increasingly hinge on decisions made and consequently, actions taken by lower echelon leaders. Success or failure will rest on their ability to make the right decision responsively and reliably. This has given rise to the phenomenon of the ‘Strategic Corporal’. To aid the networked ‘Strategic Corporal’, every soldier should be trained in critical thinking and ethical decision-making. It is essential that they have the skills to make good decisions in relation to the given context. Additionally, the commander must help ‘map’ the soldiers in context to the networked environment, where they can see their own decision-box and how it interfaces with the rest in relation to the mission outcome.

Leadership in the networked environment calls for an accentuated form of entrusting decisions to the individual soldier, and then supporting them in following those decisions. A key element of this type of leadership is effective decentralization and that requires leaders to delegate authority confidently. SAF commanders will increasingly need to deal with the diffusion of “authority and responsibility across the set of temporary and informal organizational structures that will evolve under collaboration”.³⁰ Leaders should see themselves orchestrating operations, as opposed to directing, that will bring to bear the full effects arising from the new order of decision-making, characterized by *Multiplicity*, *Simultaneity* and *Responsiveness*. It takes trust for networked forces to function efficiently. An environment of trust will promote efficient operations through parallel decision-making. Arguably, operational trust is the lynchpin in all networked operations.³¹

Conclusion

One unmistakable trend is that the nature of warfare is changing. The dawn of the networked era has unleashed a new source of power and it is *not* exclusive to anyone. As adversaries exploit networks alike, the SAF must then seek new leverage to maintain the comparative edge over them. Such leverage comes not from having superior network capabilities, but by being shrewder and quicker in exploiting information through superior decision-making. Based on the argument put forth wherein superior decision-making is borne out of a systemic consideration of *Technology, Knowledge and Command & Control*, a conceptual framework that maps the key attributes into a coherent ensemble has been proposed. Given the symbiotic relationship amongst the three domains, it is important to pursue the associated initiatives and efforts within a purposeful and coherent strategy, guided by such a conceptual framework, to *outdo*, *outthink* and *outwit* the adversary. ☺

(Ed note: This essay is the second prize winner of CDF Essay Competition 2006)

Endnotes

- ¹ Based on a report to the U.S. Congress that provided the background and oversight of NCW issues. Available: <http://www.fas.org/man/crs/RL32411.pdf>
- ² Defense Technology Area Plan. Chapter III – Information Systems Technology. Available: http://www.fas.org/spp/military/docops/defense/97_dtap/informat/ch030301.htm
- ³ Cummings, M. L. and Bruni, S., *Collaborative Human-Computer Decision Making in Network Centric Warfare* (Massachusetts Institute of Technology). Available: http://web.mit.edu/aeroastro/www/labs/halab/papers/Cummings_TTCP.pdf.
- ⁴ RAND Corporation. Research Brief. “Modern Decision Support Science Suggests New Methods and Tools to Support Military Decision Making.” Available: <http://www.>

- rand.org/pubs/research_briefs/RB177/index1.html
- 5 Cummings, *Collaborative Human-Computer Decision Making*.
- 6 <http://www.interaction-design.org/encyclopedia/satisficing.html>
- 7 This notion is consonant with a key theme of modern decision science that recognizes the need for a full appreciation of uncertainty. This gives rise to a new paradigm: Instead of seeking to “predict” effects on a system of various alternatives and then “optimizing” choice, it may be far better to recognize that meaningful prediction is often just not in the cards and that we should instead be seeking strategies that are flexible, adaptive, and robust. See Davis, Paul K., Kulick J. and Egner, M., *Implications of Modern Decision Science for Military Decision-Support Systems* (Santa Monica, Calif.: RAND Corporation, 2005), p46.
- 8 RAND Corporation. “Modern Decision Support Science Suggests New Methods and Tools to Support Military Decision Making.”
- 9 Davis, *Implications*, p55.
- 10 Defense Science Board Task Force on Training for Future Conflicts, Final Report, June 2003. Available: <http://www.acq.osd.mil/dsb/reports/tfc>.
- 11 David C. Gompert, Irving Lachow, and Justin Perkins, *Battle-Wise: Gaining Advantage in Networked Warfare* (National Defense University, January 2005). Available:http://www.ndu.edu/CTNSP/Def_Tech/DTP8%20Battlewise.pdf.
- 12 According to Lachow et al, this notion is the military equivalent of “street-wise”. It implies an intrinsic quality — some people will naturally be more battle-wise than others — but like most, if not all, cognitive abilities, it can be improved via proper training. Dr. Irving Lachow, David Gompert and Justin Perkins, “Battle-Wisdom: Improving Cognitive Performance in Network Centric Warfare”. Available: <http://www.dodccrp.org/events/2005/10th/CD/papers/295.pdf>
- 13 Gompert, *Battle-Wise*, pp23-27.
- 14 Defense Science Board Task Force on Training for Future Conflicts, Final Report, June 2003.
- 15 JFETS is designed to train the individual soldier in a decentralized, networked model of warfare in which even the lowest-ranking officer can call in an air strike or a tank battalion...The U.S. Army decided that it needed to think less about educating people on the physics of artillery tubes and start teaching them how to make smart discriminations very quickly in close urban fights. The focus is on training in cognitive decision-making rather than skills. See Steve Silberman, “The War Room”, *Wired* (Sep 2004). Available: http://www.wired.com/wired/archive/12.09/warroom.html?pg=4&topic=warroom&topic_set=.
- 16 Network theory suggests that ad-hoc teams will self-organize to deal with common problems, enabling an organization to continuously optimize its resources despite uncertainty and change. See Gompert, *Battle-Wise*, p30.
- 17 Colonel P. Forgues, “Command in a Network-Centric War”, *Canadian Military Journal* (Summer 2001), p30.
- 18 C. McCann and R. Pigeau, “Clarifying the Concepts of Control and of Command”, Proceedings of the Command and Control Research and Technology Symposium, Washington, DC: CCRP, Dept. of Defense (1999), p480.
- 19 *Ibid.*, p484.
- 20 C. McCann and R. Pigeau, “Re-conceptualizing Command and Control”, *Canadian Military Journal* (2002), p64.
- 21 Department of Defense, (2001) Joint Publication 0-2, United Action Armed Forces (UNAAF), Rev July 2001, DOD Publication No. JP-02 (Washington, DC: US Government Printing Office, 2001: V-3).
- 22 Alberts, David S., and Hayes, Richard E., *Power to the Edge: Command and Control in the Information Age* (Washington, DC: CCRP Publication Series, 2003), p6.
- 23 *Ibid.*, p218.
- 24 Accordingly, diversity of information and knowledge not only improves the quality of our decisions, but also allows us to respond and adapt appropriately to the challenges of the external environment. Alignment of decisions relates to everyone having a clear understanding about what matters, so that decisions are harmonized across all levels of the organization and reflect the current view of what collectively we know. Given the inherent characteristics of the web structure where multiple redundant paths for information sharing will be possible, decision-making can become decentralized and no longer have to occur in series. With high quality information, competent troops, trust in operations, and a clear understanding of command intent, it is possible to empower subordinates with greater decision-making responsibilities than ever before. This affords multiplicity and simultaneity in decision-making. These insights are consonant to the concept of power to the edge, which shifts the emphasis away from incremental hierarchical decision-making to liberate organizational power. See McKenzie, Jane and Winkelen, Christine, *Understanding the Knowledgeable Organisation: Nurturing Knowledge Competence* (London: Thomson Learning, 2004), pp67-83.
- 25 Gompert, *Battle-Wise*.
- 26 Adapted from Wikipedia. Available: <http://en.wikipedia.org/wiki/Satisficing>.

²⁷ Davis, *Implications*, p97.

²⁸ Gompert, *Battle-Wise*.

²⁹ Auftragstaktik is a mission-type tactic used by the Germans wherein the military commander gives its subordinate leaders a clearly defined goal and the forces needed to accomplish that goal with a time-frame within which the goal must be reached. The subordinate leader is given initiative and freedom in execution which enables flexibility in order execution. Source: Wikipedia.

Available: http://en.wikipedia.org/wiki/Mission-type_tactics

³⁰ NetCentricJointFunctionalConceptWorkshop Outbrief. July 2004. Available: <http://www.netcentricfcf.org/NCFCBWorkshop3.html>.

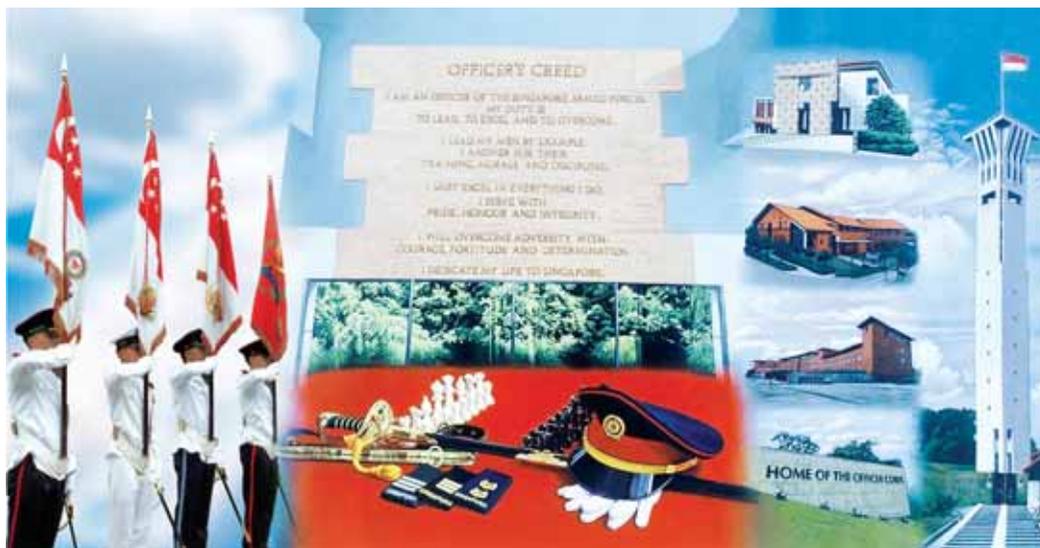
³¹ Major Nicole Blatt, USAF, "Trust And Influence In The Information Age: Operational Requirements For Network Centric Warfare", 10th International Command and Control Research and Technology Symposium: The Future of C2, 15 March 2005. Available: <http://handle.dtic.mil/100.2/ADA429673>.



MAJ Liew Hin Ban is currently a Section Head in Air Logistics Department. An Air Engineering Officer by training, he was formerly an Officer Commanding in Air Logistics Squadron, Air Defence and Systems Division, and a Staff Officer in Air Logistics Department. MAJ Liew is a recipient of the Defence Technology Training Award and he holds a Bachelor of Engineering (Second Class Upper Honours) in Electrical and Electronics Engineering from Nanyang Technological University.

Developing the Thinking Competency of SAF Leaders

by LTC Lim Choon Peng



Introduction

“While we train and hone the skills of our men and our units, we know that the next conflict is unlikely to be like the last. We have to try to envision what the next battle will be like and prepare for that, so as not to be on the receiving end of nasty surprises.

But the paradox is that what we need most to train our men in, is not to be surprised, if in spite of all the preparation and training, things do not unfold as they had expected. They must have the ability to assess the situation as it unfolds and have the

ingenuity and courage to try bold and creative solutions, even in the heat of battle, to prevail.”

RADM (NS) Teo Chee Hean
Minister for Education and Second
Minister for Defence, 2002¹

Closer to home, the events in the past few years, such as global terrorism in 2001, SARS crisis in 2003, and more recently, responding swiftly to disaster relief in Indonesia, have taught us that the SAF must be prepared to confront a wide range of threats from a number of directions and participate in a wider spectrum of operations.

The SAF operating environment has changed and will continue to change at a more rapid pace. It is envisaged that the future SAF missions *will likely be executed in a more complex, time and resources limited and uncertain environment.*

The SAF recognizes that dealing with such threats requires different capabilities and skills, and a different orientation in mindset. SAF officers and soldiers will be required to operate in situations where they may not have previously encountered and for which they haven't been trained. The ability to critically think through and solving a problem creatively, rather than applying previously learned solutions and procedures, is crucial to mission success. Hence, in 2001, the SAF initiated a major effort to review and enhance its system for leadership development. A project team was established to map out the scope of leadership thinking or doctrine, and a system for leadership development in the SAF. In 2003, this project team was centralized in an interim organization called the "Centre of Leadership Development" or CLD.

CLD's significant achievements include the conceptualization of the new SAF Leadership Framework and a new behavioral Leadership Competency Model (LCM) for the Officers, Warrant Officers and Specialists in the SAF.

As endorsed by the SAF senior leadership, one of the core competencies desired for a SAF leader is the "Conceptual Thinking" ability. Conceptual Thinking is the cognitive capacity to understand and respond to the complexities inherent in the SAF operating environment, including making sense of the moral and ethical dilemmas that may arise.²

The objective of this paper is to provide a discourse on developing conceptual thinking skills in SAF leaders. The approach of the paper is to provide the theoretical foundation on "what is thinking" and a description of "thinking" in the context of the SAF. It will then be followed by a description on the gaps and possible approach suggestions to develop the thinking skills of the SAF leaders. This paper will

Competencies	"Core Competencies" (For Leader Performance)				"Meta-competency" (For Growth/ Adaptability)
	Conceptual Thinking	Social	Mission	Development	Self
Skills	Critical Thinking	Communicating to influence	Planning	Developing People	Self Awareness
	Creative Thinking	Interpersonal Effectiveness	Decision Making	Developing Team	Self Management
	Ethical Reasoning		Execution	Improving Organization	Personal Mastery

Table 1. SAF Leadership Competencies and Skills.

address specifically the subject of critical and creative thinking in the SAF.

What is “Thinking”?

As one explores the literature about thinking, you will discover that the definition or description of thinking is complicated. There are different views, types, forms, styles, degrees (order) and levels of thinking that are stated by different gurus ranging from early philosophers such as John Dewey to modern practitioners in the likes of Edward De Bono. A simple and clear way of describing thinking is stated by Robert Boostrom.³ In its loosest sense, thinking signifies everything that, as we say, is “in our heads” or that “goes through our minds”. In this sense, you are always thinking about something, including daydreaming. In a narrower sense, thinking is a matter of bringing things to mind things that you cannot see or hear. This sort of thinking is different from daydreaming because it involves some effort and it has a goal. Telling a story is a good example of this sort of thinking. You try to recollect events as it actually happened and sorting out the events into an order or pattern. In a narrower sense, thinking is an expression of beliefs based on evidence. Someone asks you what you think about an issue and you say what you believe. Finally, there is a kind of thinking that you do when you are looking for reasons for believing one thing instead of another. When you do this kind of thinking, you look not for any evidence, but for good evidence. This kind of thinking is sometimes called reflection. When you reflect, you are *thinking actively, persistently and carefully*.

The quality of one’s thinking is dependent on traits (inborn), behavior (which is shaped by culture and experiences) and the educational system. Thinking is a skill just like driving a car or cooking, in which some are better than others. The will to improve has to come first, followed by attention and practice. At first, it seems awkward and unnatural, but as time progresses, the fluency and effectiveness of one’s thinking will improve.⁴

Types of Thinking

There are many types of thinking skills that exist today that differ largely on the context in which it is applied. There are thinking skills such as Critical Thinking, Creative Thinking, Ethical Reasoning, Abstract Thinking, Lateral Thinking and System Thinking. Within the scope of this paper, critical thinking and creative thinking will be discussed further.

Critical Thinking

Everyone thinks; it is our nature to do so. But much of our thinking, left to it, is biased, distorted, partial, uninformed or prejudiced. John Dewey described this mode of thinking as “unreflective” thinking – it occurs when one jump to conclusion quickly, accepts claims at face value without really thinking about it. On the contrary, reflective thinking is an active, persistent and careful thinking process.⁵ “*Reflective Thinking*” is one of the early terms coined by John Dewey to describe this form of thinking, in which modern practitioners used synonymously with “*Critical Thinking*”.

Michael Scriven, a modern practitioner defined “*Critical Thinking*” as the mode of thinking about any subject, content, or problem, in which the thinker improves the quality of his or her thinking by skillfully taking charge of the structures inherent in thinking and imposing intellectual standards upon them.⁶

Critical thinking can be seen as having two components: 1) a set of information, belief generating and processing skills, and 2) the mental disposition during engagement. It is not mere acquisition and retention of information alone, because it involves a particular way in which information is sought after and treated. It is not mere possession of a set of skills, because it involves the continual use of them to guide behavior. Peter Facione summarized the set of information processing skills and disposition in the following graphic illustrations.⁷

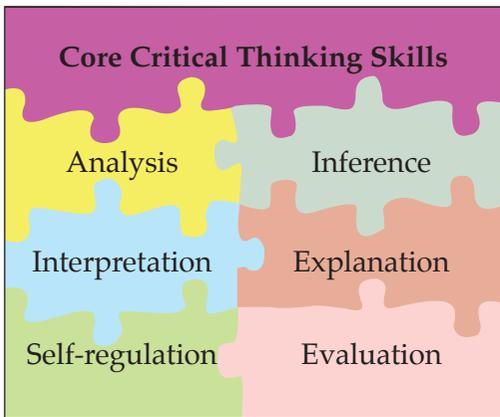


Figure 1. *Critical Thinking Skills.*

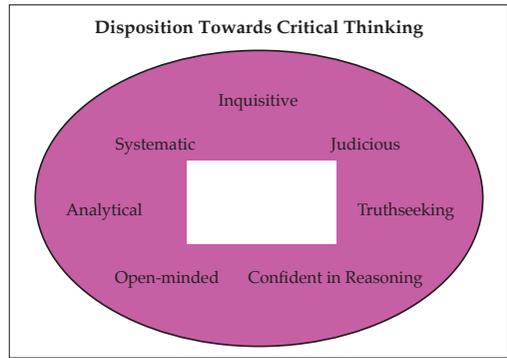


Figure 2. *Mental Disposition towards Critical Thinking.*

The attributes of a well-cultivated thinker are:

- Raises vital questions and problems, formulating them clearly and precisely;
- Gathers and assesses relevant information, using abstract ideas to interpret them effectively and arriving at well-reasoned conclusions and solutions, testing them against relevant criteria and standards;
- Thinks open-mindedly within alternative systems of thought, recognizing and assessing, as need be, their assumptions, implications, and practical consequences; and
- Communicates effectively with others in figuring out solutions to complex problems.

Creative Thinking

“Creativity is inventing, experimenting, growing, taking risks, breaking rules, making mistakes, and having fun.”

- Mary Lou Cook

Much of the thinking done in formal education emphasizes the skills of analysis – teaching students how to understand claims, follow or create a logical argument, figure out the answer, eliminate the incorrect paths and focus on the correct one. However, there is another kind of thinking, one that focuses on exploring ideas, generating possibilities, *looking for many right answers rather than just one.*⁸ Creative thinking is defined as the process of exploring multiple avenues of actions or thoughts. Sometimes, it is also called divergent thinking because thought patterns or areas of beliefs are expanded to increase the likelihood of new thoughts or ideas occurring.

Relationship between Critical and Creative Thinking

“The critical and creative functions of the mind are so interwoven that neither can be separated from the other without an essential loss to both.”

- Anonymous

Critical and creative thought are both achievements of thought. Creativity masters a process of making or producing, critically a process of assessing or judging. Imagination and reason form an inseparable team.⁹

What is “Thinking” in the Context of the SAF?

How do leaders in the SAF think? It is hard to quantify the type and level of thinking in the SAF, short of conducting a SAF-wide survey. However, some common attributes of a military mindset as perceived by others (i.e. not serving

in any military establishment), could be used to frame the intellectual argument. One narrow view suggested that the military mindset is often characterized by conventional thinking, lack of imagination, unwillingness to challenge accepted doctrine, excessive caution, professional pessimism, narrowness of outlook, and subservience to the views of higher authority.

One argument that supports this perception looks at the environment in which the SAF operates. The SAF operates in a unique environment in which it has never been called to war or faced severe crises that challenged its survival. Also, the perceived threats and plans to counter the threats have not changed significantly, at least in the period before 9/11. Lastly, it has large, adequate and fixed resources to operate year after year without having to worry about sustainability. Plans and processes within the SAF are revised and optimized to its best efficiency without many changes to its intent and context. These environmental features foster a certain behavior in the SAF psyche. There is no real impetus for leaders in the SAF to think and innovate.¹⁰ Superior officers accept plans that are routinely developed based on the previous “master” copy, since most of the considerations have already been thought about. Exercises are “routinized” into standard operating procedures and are practiced diligently. Lessons learnt are meticulously incorporated into checklists with a narrow focus on the “how” to do it more efficiently or effectively, rather than understanding the “what” and “why” and the context in which it was applied. Processes are



Crew of RSS Vengeance, winner of the Best Ship Award 2007; organizations with confident leaders, more competent thinkers, coupled with open climate, will be able to progress further in developing and demonstrating thinking competency.

highly structured and efficient, and coupled with past successes, it has led to the development of *mental complacency* among leaders in the SAF.

As a counter-argument to this perception, there is also definitive evidence that portrays the SAF as a “thinking and innovative” organization. Firstly, the educational profile (ranging from PhD to diploma holders) of leaders that the SAF has and recruits every year, provides an impressive yardstick on the thinking capacity of its leaders. Secondly, the SAF offers an impressive range of scholarships, training awards and development courses for its officers and WOSA corps. The leaders that the SAF sends for such courses often return with merit awards and commendations from the overseas academies or institutions. This reflects the quality of people we have in the SAF. Thirdly, the impressive results achieved in the operational arena

[such as participation in Peace Support Operations (PSO) and Operation Flying Eagle], the organizational excellence arena [such as Singapore Quality Award (SQA) and Innovation Class] and in the literacy arena (quality of entries in the CDF Essay Competition and *POINTER* journal), provide evidence of “thinking and innovative” people in the SAF.

So which is the accurate perception of “thinking” in the SAF? The short answer is that there is no consensus and it really depends on the context, personal experiences and where you are in the leadership level. Organizations within the SAF that are filled with confident leaders, more competent thinkers, together with a more open climate, will be able to progress further in developing and demonstrating thinking competency, while others with limited resources and a suppressed climate will not fair as well as others.

What are the Gaps?

SAF leaders must learn to think beyond the boundaries of their physical surroundings. They have to think creatively, search for new knowledge and come up with new ideas, tactics or solutions against future threats. However, there are inherent gaps that may hinder the development of these crucial thinking skills in the SAF. They are the Singapore education system and the organizational culture.

Singapore Education System

“Singapore has a strong education system and one that is widely recognized for having produced generally high levels of academic achievements among students. However, there has been a concern among the political leaders with regards to the kinds of students produced by the system. The general perception is that the system was producing students who were muggers rather than critical and creative thinkers.”¹¹

Mr. David Chan
Director, School of Information &
Communications Technology
Ngee Ann Polytechnic

Mr. Chan attributed the lack of critical and creative thinking skills to the traditional education methodology that was used before 1997. Often the information the teacher disseminates to students is directly aligned with the information offered by the textbooks. Students are provided with only one fixed view of complex issues and one set of truths. Although there is a growing interest in cooperative learning, most classrooms structurally discourage

cooperation and require students to work in relative isolation on tasks that require very little higher order thinking skills. When asking students questions, most teachers want the right answers rather than encouraging students to think through intricate issues. Schooling is premised on the notion that there exists a fixed world that the learner must come to know. The construction of new knowledge is not as highly valued as the ability to demonstrate knowledge of conventionally accepted understandings.

In 1997, the Ministry of Education undertook a fundamental review of its curriculum and assessment system to see how the schools can better develop the creative thinking and learning skills required for the future. Schools were encouraged to move students away from a mere mastery of content and to emphasize instead learning and thinking skills.¹²

Most of the leaders in the SAF today belong to the pre-1997 era, where education is based mainly on mere mastery of knowledge rather than thinking skills. Except for a privileged few who have pursued tertiary education locally or overseas, the critical and creative thinking skills competency of the general population in the SAF is arguably limited.

Organizational Culture

The hierarchical military structure is necessary for the SAF to perform its primary role with efficiency and effectiveness, but it also poses special challenges towards the development of

creative and critical thinking in the SAF. In a typical military structure, soldiers are trained to follow orders without questions. Mistakes are not tolerated and punishment is swift for non-conformity. Risk could be minimized by strict adherence to Standard Operation Procedures (SOP). Innovative variation to training methods with a small risk of affecting training objectives is not welcome. Superior officers assume that they know everything and are fully aware of what needs to be done. Similarly, subordinates also assume that their superior officers know what to do and their jobs are to take directions from them. Questioning the superior is seen as being disrespectful and the individual concerned may even be labeled as a “trouble maker”. Therefore, this created a disposition towards an *unquestioning mindset*. In addition to

these cultural blocks, there exists a “fast-food” culture in the SAF, which short-circuits the thinking process. SAF leaders want quick results with minimal thinking – “no need to think, just do it” mentality.¹³ Arguably, the military organizational culture may have inevitably created some gaps in development of thinking competency among its SAF leaders.

How to Develop Thinking Skills in the SAF?

The key concepts from “theory of thinking”, “thinking within SAF” and “inherent gaps”, were extracted and rearranged according to common attributes and patterns. The outcome is the distillation of three factors that has a direct effect on developing thinking competency in SAF leaders.

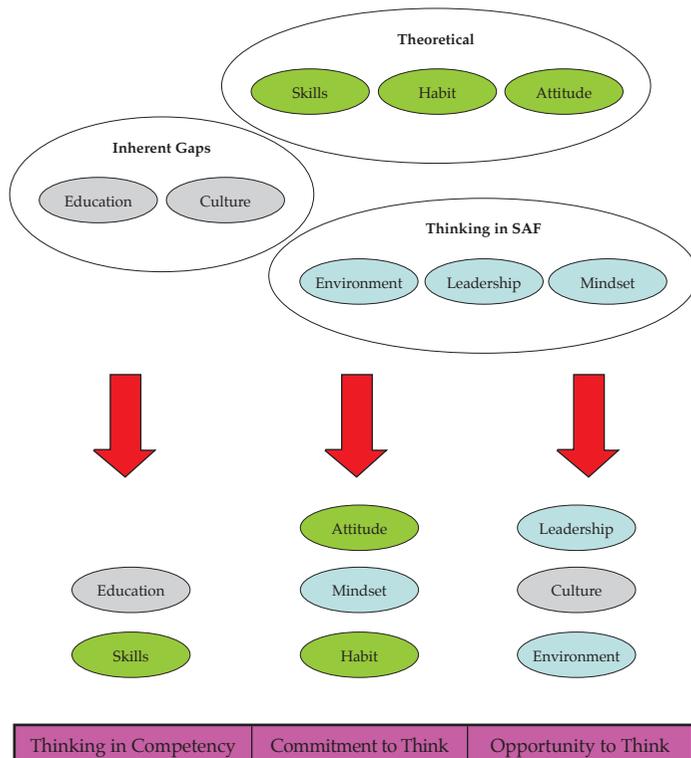


Figure 3. A Snapshot of the Thinking Framework.



Figure 4. An Illustration of the Intellectual Power Equation.

These three factors, which is “Thinking Competency”, “Commitment to Think” and “Opportunity to Think” were combined to form the *Intellectual Power Equation* as illustrated above.

The main strategy for development of thinking skills in the SAF leadership is to maximize the intellectual power among SAF leaders. This power provides greater capacity for SAF leaders to make sense of the complex environment and make swift and superior decisions.

The SAF offers an attractive range of scholarships and training awards, coupled with good remuneration packages, to recruit the best talent

available. The SAF also provides a vast array of self-improvement training and leadership development courses for its leaders, thus providing the best education for its leaders. In addition, the educational profile of national servicemen has significantly improved and will continue to improve. Therefore, the main challenge is not the lack of “thinking competency” in the SAF leadership. The main challenges that the SAF needs to address are 1) providing the “Opportunity to Think”, which is largely dependent on leadership, environment and culture, and 2) instilling this “Commitment to Think” among its leaders, which involves changing the people’s mindset.

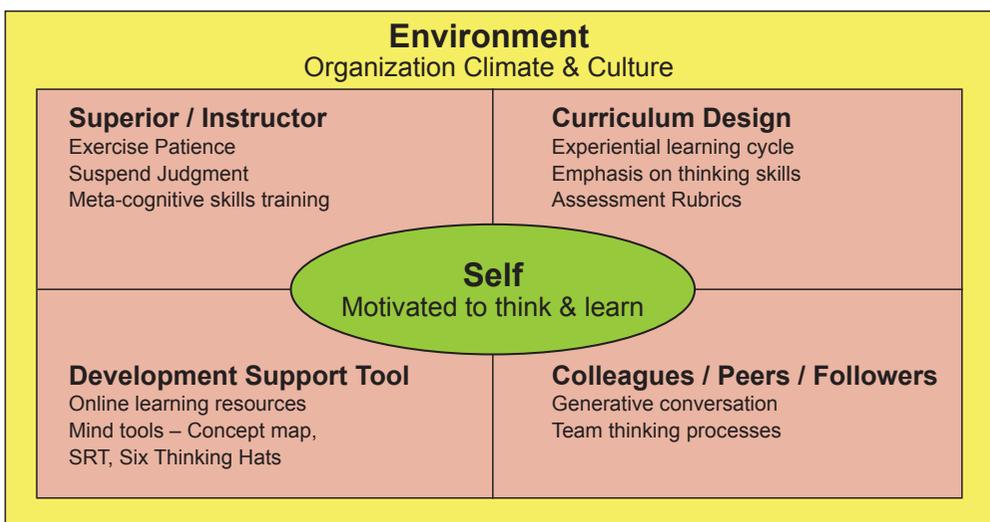


Figure 5. The Thinking Climate and Culture Framework.

One suggested approach to develop thinking skills in the SAF leadership involves the six components as illustrated in the diagram 5.

Component 1: The Self

“Self” is at the core of the leadership’s thinking skill development. This component refers to an individual personal commitment in the developmental process. SAF leaders need to change their mindset about the quality of their “thinking”. *It is not about past academic achievements but more of an attitude and habit (mindset) that will produce good thinkers.* They need to be aware of what constitutes “good thinking” and takes ownership to improve their thinking competency. They need to have an inquisitive mind to ponder, a critical mind to think through, and a creative mind for problem solving or decision-making. One of the best ways to “grow” your intellectual mind is to read widely, read wisely and read differently.¹⁴ Personal reflection and engaging in generative conversation will also help to keep the thinking mind active.

Component 2: Environment

This refers to the immediate organizational culture/climate and to the extent in which it is conducive for thinking, learning, change and growth. The SAF has adopted the “Learning Organization” (LO) framework and has been promoting it actively in SAF academic and vocational schools. Useful concepts and tools such as check-in/check-out, rules for quality conversations, deep listening and reflection, aids in providing the right

climate and opportunity to engage in generative conversation and quality thinking. This LO framework needs to propagate beyond classrooms and be practiced diligently in SAF units.

Component 3: Superiors and Instructors

Superiors and instructors have direct influence over their trainees and subordinates, and therefore, have natural impact on their thinking skill development. Superiors need to be open-minded, exercise patience and suspend judgment when engaging their subordinates during discussion. They need to encourage their subordinates to think through intricate issues and resist the urge to dictate instructions. Instructors need to be trained with meta-cognitive skills to recognize different thinking patterns and should be competent to teach thinking skills.

Component 4: Peers, Colleagues and Subordinates

Besides the individual’s reflection, thinking skills is developed most actively during generative conversation with peers, colleagues and subordinates. SAF leaders should engage actively with peers and subordinates to discuss larger issues besides work alone. They should build trust and encourage each other to share their individual perspectives on complex issues. Listening and communication skills that are acquired from LO could be used to foster greater understanding, to build trust and, more importantly, to sharpen one’s thinking skills through active engagements.

Component 5: Curriculum Design

A key process in thinking development is the experiential learning cycle, which calls for thinking development to be infused into everyday life activities, in our training schools and units, rather than as isolated events or activities. As far as possible, training curricula should be designed to connect abstract concepts with active experimentation, concrete experience, reflective thinking and observation. In addition, the curriculum design could also include training in meta-cognitive skills, critical and creative thinking skills. This will allow students to recognize their style and level of thinking. The desired outcome is for students to take ownership and improve their thinking proficiency.

Component 6: Developmental Tools and Procedures

A thinking organization provides powerful process tools designed to tap into the thinking power of its people. These process tools provide a common set of frameworks and language for the necessary thinking and discussions for people to engage in, in order to derive good solutions. Examples of such tools are concept mapping, mind mapping, decision making tools, problem solving, brainstorming, Six Thinking Hats, SRT, etc. They need to be made readily available in units or through the OA system.

Conclusion

“The nurturing of the SAF intellectual mind is not the responsibility of academies and colleges only but of leaders everywhere.”

This paper provided some simple understanding on “what is thinking” and offers two perceptions of “thinking” in the SAF. Two inherent gaps, namely the Singapore education system (before 1997) and the prevailing organizational culture were identified as hindrances. Finally, a main strategy and a system approach were suggested to develop the thinking competency in the SAF leadership.

Since 2001, the SAF has taken steps to focus on leadership development. There is now greater clarity and understanding of what the desired competencies of a SAF leader are. However, as efforts are ongoing in developing the course curriculum and shaping leaders’ mindset throughout the SAF, there is a need to explore these individual competencies in greater depth. Such exploration efforts may reveal the current gaps and nuances in the SAF that may help to foster better understanding of the issues. 

(Ed note: This essay is the third prize winner of CDF Essay Competition 2006)

Endnotes

- ¹ Excerpt of speech by RADM (NS) Teo Chee Hean, Minister for Education and Second Minister for Defence at Foundation Stone Laying for Changi Naval Training Base, Jan 2002.
- ² Extracted from “SAF Leadership Competency Model (LCM)” LD DOCTRINE DIRECTIVE 3/2004 dated 26 Jul 04.
- ³ Robert Boostrom, *Developing Creative and Critical Thinking Skills* (National Textbook Company, Lincolnwood, Illinois, USA, 1993).
- ⁴ Edward De Bono, *De Bono Thinking Course* (Facts on File Publication, Oxford England, 1985).
- ⁵ John Dewey, *What is Thought?* (Lexington, Mass: D.C. Heath, 1910), pp1-13.
- ⁶ Michael Scriven and Richard Paul, *Defining Critical Thinking*, available at <http://www.criticalthinking.org/aboutCT/definingCT.shtml>

- ⁷ Peter A. Facione, *Critical Thinking: What it is and Why it Counts* (California Academic Press, 1998).
- ⁸ Robert Harris, *Introduction to Creative Thinking*, available at <http://www.virtualsalt.com/crebook1.htm>
- ⁹ Dr. Richard Paul and Dr. Linda Elder, *Critical and Creative Thinking* (Foundation for Critical Thinking, 2004).
- ¹⁰ Extracted partly from the opening address by Mr Eddie Teo, Chairman of the Steering Committee for an Innovative Public Service at Deep Dive: A Symposium for Activists on 20 February 2003, available at <http://www.ps21.gov.sg/challenge/200304/coverstory/speech.html>
- ¹¹ David Chan, “The Role of ICT in a Constructivist Approach To the Teaching of Thinking Skills”, e-library CLD, SAFTIMI.
- ¹² Schools were asked to cut back on the amount of content knowledge that students are required to learn. Teachers were also encouraged to spend more time on projects that can help develop thinking skills.
- ¹³ LTA Benjamin Cher Tau Wei, “A Learning Army – Translating Theory into Practice”, *POINTER* Vol.29 No.1 (2003).
- ¹⁴ LTA Kwan Choon Tuck, “Reading and Growing” *POINTER* Vol.25 No.4 (1999).



LTC Lim Choon Peng is currently a Branch Head in Air Plans Department. An Air Engineering Officer by training, he was formerly a Section Head in Air Logistics Department and an Officer Commanding in Air Logistics Squadron, Sembawang Air Base. LTC Lim is a recipient of the Defence Technology Training Award and the SAF Postgraduate Scholarship. He holds a Bachelor of Engineering (Second Class Upper Honours) in Mechanical Engineering from Nanyang Technological University and a Master in Aeronautical Engineering from Naval Postgraduate School, USA.

Software Defined Radio Design for an IEEE 802.11a Transceiver using Open Source Software Communications Architecture (SCA) Implementation::Embedded (OSSIE)

by MAJ Leong Wai Kiat, Chris

Abstract

A military unit will not always know in advance what communications capabilities it will need in operations. This is especially true in coalition operations, where the coalition partner's forces may not have the preferred radio equipment. Therefore, in operations, it is imperative to be prepared for many different means of communications, especially those that a coalition partner would be likely to possess. Radio equipment built to commercial (i.e. IEEE wireless) standards is a likely means of communications. Software Defined Radio (SDR), with the software to communicate in many modes, including commercial standards, would be a substantial advantage to a military unit that is part of a coalition operation, when time and foresight may not be sufficient for the fielding of communications equipment ideally suited for the specific coalition membership. For this research, the focus is on software design for the commercial standard IEEE 802.11a implemented on a SDR.

In this thesis, the author presents the design of a SDR transceiver using Open Source Software Communications Architecture (SCA) Implementation::

Embedded (OSSIE) as the software platform. Designing a SDR requires both an appreciation of the IEEE 802.11a (wireless Local Area Network at 5 GHz band) protocol standard as well as the understanding of the C++ and Common Object Request Broker Architecture (CORBA) software tools available to implement the physical transmitter and receiver layers. For this work, the Incremental Development Model was chosen, and it comprises of three stages: Design, Develop and Verify. The advantage of this model is its incremental nature, which allows the developer to learn from earlier versions of the system. The completed transmitter and receiver layers are validated successfully according to test cases stipulated in the IEEE standard.



Figure 1. Forest fire rescue mission – a time critical coalition operation.

Introduction

“A major forest fire has occurred in the country. This fire has spread out of control and has forced a number of local communities to evacuate as the fire approaches their homes and offices. Fire fighters and other emergency responders from organizations and jurisdictions nation wide have responded to this emergency, with each group bringing their own equipment. Unfortunately, the radio equipment from the various jurisdictions are not interoperable with each other or with the civilian radio infrastructure, and this lack of interoperability is causing a huge problem in coordinating efforts. Without a way to allow these various radio equipment to interoperate, this lack of coordination has put the responders at risk, and has forced many front line responders to carry several radios to allow an appropriate level of inter-organizational communication.”

*Extracted from SDR forum –
Smart Radio Challenge, Nov 2006*

The above scenario, extracted from the Software Defined Radio (SDR) forum, could easily have been applied to the SAF, for example, the coalition operations during the Tsunami Humanitarian Assistance and Disaster Relief missions in 2004. This is an excellent motivation for the focus and resources that have been channeled to current design and development of SDR. The need for an interoperable radio set that remains flexible and modular during operations will definitely enhance mission success.

Reed defines a SDR as a radio that can be “substantially defined in software and whose physical layer behavior can be significantly altered through changes to its software”¹. SDR has advantages over conventional radio as it promotes multi-functionality, mobility, compactness, ease of manufacture and ease of upgrades.

Military Applications

SDR has found itself in numerous military applications from the early adopter like the SPEAKEasy to the current Joint Tactical Radio System (JTRS). The JTRS has a close linkage with the United States Department of Defense’s information framework known as the Global Information Grid (GIG). The capabilities of the JTRS serve as enablers for the GIG’s transformational networking to reach out from the command center level to the actual mobile military nodes.

The JTRS was established in early 1997 in response to the military pursuit of programmable, modular, multi-mode, multi-band radio to replace existing legacy radios. It eventually evolves from a radio replacement program to a networking program to support the GIG. With this emphasis, the Joint Program Executive Officer (JPEO) for the JTRS program was formed in February 2005. This reinforced the importance of tapping the evolving SDR technology available and converting this technology to military war fighting capabilities through the JTRS acquisition program. One good example is the Digital Modular Radio (DMR) developed by General

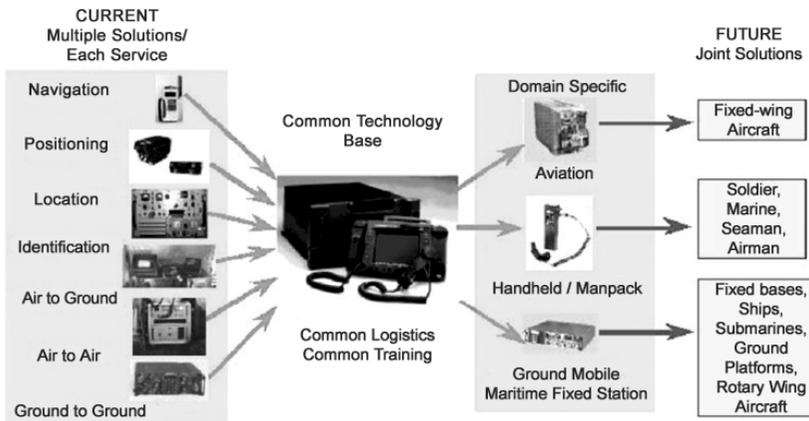


Figure 2. JTRS – A multi-mode, multi-band SDR.

Dynamics that is in the process of complying with SCA so as to incorporate JTRS JPEO-provided waveforms to meet operational requirements.

Guiding Principles

Designing a SDR requires both the appreciation of the protocol standard as well as the understanding of the software tools available to implement the physical transmitter and receiver layers (layer 1 under the OSI 7 layers model). In order to implement the coding effectively and efficiently within the limited amount of time, it is important that the whole research should be conducted with a set of guiding principles in mind. The following three are singled out as critical factors guiding the research that has been carried out.

1. Start Small

Implementing the IEEE 802.11a physical layer using OSSIE requires a total of 23 components, 12 different functionalities and 31 sequential

input-output (I/O) processes for the transmitter, while the receiver is implemented with 18 components, 12 different functionalities and 20 sequential I/O processes. It would be a daunting task to jump straight into the coding of a full-scale IEEE 802.11a standard as it is extremely complex and would probably result in a demoralizing outcome.

Hence, the strategy is to ‘start small’ by first developing simple components that work. This will help to build up confidence and experience in using the OSSIE software, which is still a trial version. This assimilation time is needed to understand the programming language and flow. An Incremental Development Model has been chosen for the software implementation as it advocates the need to be modular and provides constant feedback in the design cycle to minimize back tracing. It minimizes major bugs from occurring in the design further downstream in the implementation. More details on the model are provided later.

2. Think Modular

As this research is more of a discovery venture (since it is the first time an attempt has been made to use OSSIE to implement IEEE 802.11a standards), the push for a direct working design outweighs the need for an efficient one. Hence, it is more important to get the various components under the standard to carry out their necessary functions, even though the code may not be written as efficiently as desired. If there is a need, future efforts can be recommended to optimize the code and integrate it with other aspects of the standards or hardware. These further enhancements are proposed in the concluding section.

The targets to be modular and reusable reinforce the need to keep the components ‘simple’ so that they can be understood and modified easily for future enhancement. While the OSSIE waveform developer already provides handy tools to modify components, it is critical to have good programming discipline in managing the complexity of the software algorithm. This prevents the code from getting too exclusive and losing the flexibility of customization.

3. Help is Out There

As mentioned before, OSSIE is still under development and refinement. It is very important that one is kept up to date regarding the OSSIE software development to fully utilize its capabilities. Through the research, the author has been fortunate to have constant dialog and guidance from the OSSIE development team at the Virginia Polytechnic Institute and State University (Virginia Tech).

The algorithms, functions and objects in the software are written in the C++ programming language. However, it is equally important to appreciate the underlying CORBA interfaces that enable input/output (I/O) interaction between components and integration of the transmitter and receiver waveforms. Another challenge will be to understand the IEEE 802.11a communication standard (e.g. modulation, error corrections, orthogonal frequency division multiplexing) and convert that into the desired algorithms in the C++ programming language.

To fully understand the various technical details and challenges on one’s own is nearly impossible in such a short time. It has been important to seek assistance quickly whenever the implementation reached an obstacle. Proven algorithms and approaches are referenced so as not to reinvent the wheel. This research is also a collaboration with MAJ Low Kian Wai, who was working on the IEEE 802.16 implementation using OSSIE. Various useful resources include literature studies, Internet research, sample C++ software algorithms, MATLAB simulation for IEEE 802.11a standard, etc. All of these resources come disjointed but they provide guidance and the tools to complete the thesis research.

Software Radio Techniques

The design of a SDR generally comprises a series of procedures that include system engineering, RF chain planning, Analog-to-Digital and Digital-to-Analog hardware selections, software and hardware architecture selection and radio validations. In this thesis research, the focus is on the software architecture

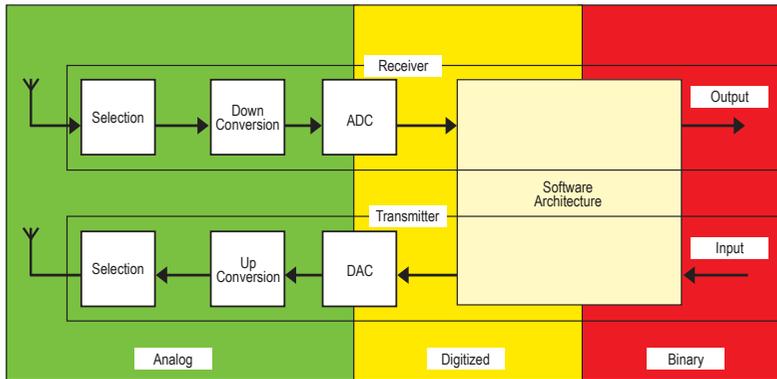


Figure 3. Model of Software Defined Radio.

and the transceiver components shall be implemented using software radio techniques.

The components will be designed for use in an IEEE 802.11a transceiver and for contribution to the library of components being developed. The components developed shall be flexible so that they can be modified to implement other receivers by customizing the appropriate parameters. Design of the SDR shall use SCA including CORBA for flexibility, performance and maximum potential for software module reuse. The components shall be tested based on functions and test cases found in the IEEE 802.11a standard.

The extent of software architecture or the boundary where software algorithms shall be written is shown in Figure 3.

For the transmitter, all functionalities from the input binary data to the digitized input to the Digital-to-Analog Converter (DAC) will be implemented in software. Similarly for the receiver, all functionalities after the Analog-to-Digital Converter (ADC) to the regeneration of the binary received information will be implemented in this thesis work. It is important to note that all software components are implemented at base band, that is, before up-conversion at the transmitter and after down-conversion at the receiver.

IEEE Standard: 802.11a

The physical standard takes reference from Part 11: IEEE Std 802.11a-1999 (Revision 2003).² It describes the wireless LAN Medium Access Control

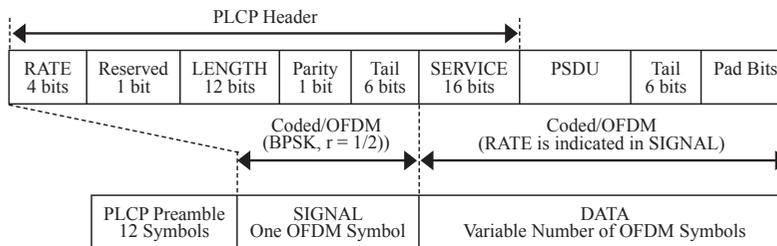


Figure 4. IEEE 802.11a PPDU frame (extracted from Standard).

(MAC) and Physical Layer (PHY) specifications, specifically for high-speed physical layer in the 5 GHz band. Since the implementation is done at base band, the carrier frequency of approximately 5 GHz band is immaterial. IEEE 802.11a is based on Orthogonal Frequency-Division Multiplexing (OFDM) whereby a single transmission is encoded into multiple sub-carriers. Section 17 of the standard (OFDM PHY specification for the 5 GHz band) is the working document upon which this thesis's algorithm is based. A simplified explanation of the working of the OFDM PHY layer can also be found in Gast.³

Important design requirements of an IEEE 802.11a PHY system are as follows:

- a) data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mbits/s
- b) mandatory transmitting and receiving at data rates of 6, 12, and 24 Mbits/s
- c) 52 sub-carriers that are modulated using binary or quadrature phase shift keying (BPSK/QPSK), 16-quadrature amplitude modulation (QAM), or 64-QAM.
- d) forward error correction coding (convolutional coding) with a coding rate of 1/2, 2/3, or 3/4. Viterbi decoding will be implemented at the receiver.
- e) 1 OFDM symbol per 4 μ s (250,000 sym/s)

Open Source SCA Implementation::Embedded

The Open Source SCA Implementation::Embedded (OSSIE) is developed by the Mobile and Portable Radio Research Group (MPRG) at

Virginia Tech as an open source SCA Core Framework solution. OSSIE was created to meet the need for a C++-based, open source SCA implementation that could be modified and adapted in a research environment. The current version of OSSIE (0.5.0) is based on version 2.2.1 of the SCA specification. A detailed presentation of the OSSIE platform can be found in Jacob A. DePriest's thesis.⁴ From his thesis, the reader would be able to appreciate the OSSIE Waveform Developer (OWD) environment.

This thesis is written with the assumption that the reader has certain prior knowledge about the C++ programming language, including object-oriented design. There are four important C++ files generated for each new component: *<Component Name>.h*, *<Component Name>.cpp*, *port_impl.h* and *port_impl.cpp*. These are where the functionalities are defined for the component. The content of these generated C++ files are modified to provide the actual functionality of a radio component.

Incremental Development Model

The intent of this model is to develop a software system incrementally, allowing the developer to take advantage of what has been learned in earlier versions of the system. The process starts with a simple implementation of a subset of the software requirements and iteratively enhances the evolving versions until the full system is implemented. At each iteration, design modifications are introduced and new functional capabilities are included.⁵ The incremental development model has

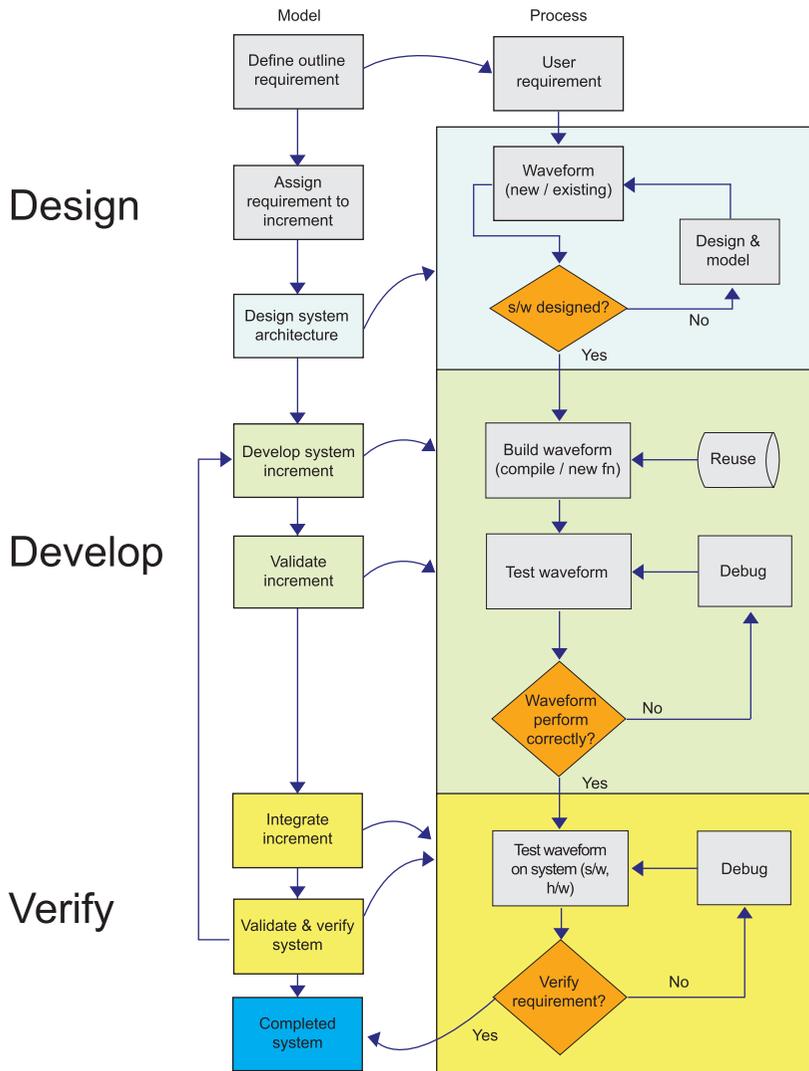


Figure 5. Incremental Development Model.⁶

three stages: Design, Develop and Verify. Figure 5 describes the interrelationship between these three stages as a model and how it corresponds to processes in the software waveform development of the IEEE 802.11a standard.

1. Design

This stage starts with defining the outline software requirements and assigning these requirements to

the specific increment. From these requirements, the system architecture is designed to serve as a framework for actual software development in the next stage.

2. Develop

This is the actual ‘hands on’ of software development and programming, whereby the system requirements and pseudo-codes are converted to actual software languages.

The coded algorithms are validated incrementally to ensure they meet the functionality expectations. Successful increments are stored for future use and new functionalities through design modifications are introduced for the next increment.

3. Verify

With the incremental development, the software system design gets larger and more complex. Increments shall be integrated in this stage and verified that the system as a whole is able to meet the holistic software requirements. For this research, the completed system must be able to emulate the IEEE 802.11a physical layer for both the transmitter and the receiver.

Following the principle of iterative and incremental development, five models have been developed, with each being more complex and built on the experiences gathered from the previous. The first three are exploratory models using MATLAB, which are relatively easy to build since many of the radio functionalities are already available as function calls. An OFDM transmission design was implemented using MATLAB according to the source code recommended by Hiroshi and Ramjee⁷. The fourth model builds on the success of the MATLAB design. It emulates a Transmitter-Receiver (Tx-Rx) design using OSSIE but following closely the previous MATLAB model. The final model is the full scale OSSIE implementation of IEEE 802.11a PHY layer, which is the primary objective of this thesis work. A summary of the models is provided in Figure 6.



Figure 6. Incremental Conceptual Design.

The OSSIE IEEE 802.11a PHY Layer Design

The full scale 802.11a PHY layer is based on the IEEE standard 802.11a-1999 (Revision 2003). There are two core system architectures – transmitter and receiver. Both are implemented in software under the OSSIE Waveform Development (OWD) environment. The types of component needed for the transmitter are described in the components flow diagram of Figure 7.

The transmitter converts the binary inputs (especially the PSDU information from the MAC layer) into digitized PPDU frames to be passed through the DAC before up-conversion for RF transmission. The PPDU frame can be subdivided into three ‘sub-frames’, namely PLCP preamble (or just Preamble), PLCP header excluding SERVICE (or just SIGNAL) and DATA. These represent the three separate ‘modules’ that shall be developed and appended to form the eventual transmitter PPDU frame. The components are developed either to carry out specific functions or to form the frames/sub-frames.

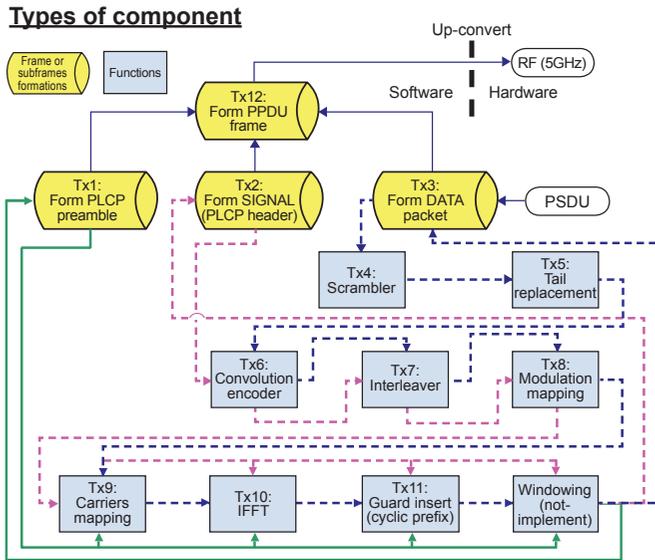


Figure 7. IEEE 802.11a Transmitter Components Flow Diagram.

The receiver carries out almost the inverse functions of the transmitter. The types of components needed are described in the components flow diagram of Figure 8. In the receiver, digitized PPDU frames (passed down from the ADC after down-conversion from the RF front end) shall be converted into binary outputs from which the original PSDU information can be extracted. Like the transmitter, the receiver is comprised of three separate ‘modules’, namely Preamble, SIGNAL and DATA sub-frames. In comparison, fewer components are needed to implement the receiver than transmitter, but the receiver entails more complexity in the C++ algorithm.

Develop and Verify: An Example

As the development and verification of the components are tedious and complex software processes, this section would only describe one such component

as an illustration of the approach. One excellent example is the Viterbi decoder component implemented under the Receiver design known as *DATA_conv_dec* (the Rx6 convolution decoder block shown in Figure 8). Rorabaugh⁸ provides a good description on how communication system can be simulated in C++ language and is adopted in this implementation.

DATA_conv_dec has one input port and one output port. The input port is linked to the *DATA_deinterleaver* component, while the output port is linked to the *DATA_descrambler* component. Viterbi decoding is chosen to decode the stream of convolutional bits as it is the preferred approach for convolutional decoding. The received bits have been coded with a convolutional encoder of various coding rates depending on the transmitted data rate. As higher coding rates are derived by employing puncturing at the transmitter, conversely, at the receiver,

Types of component

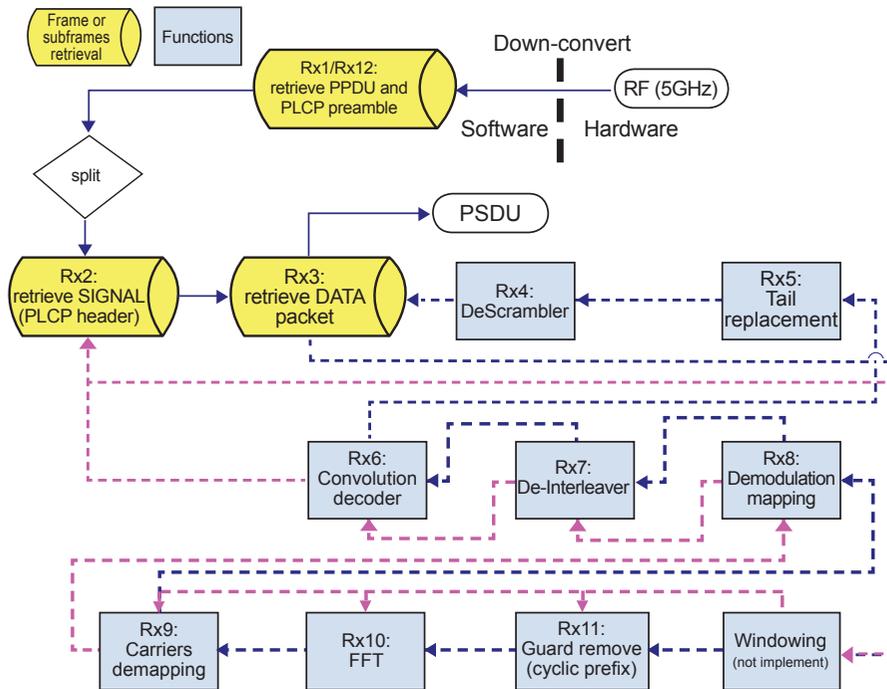


Figure 8. IEEE 802.11a Receiver Components Flow Diagram.

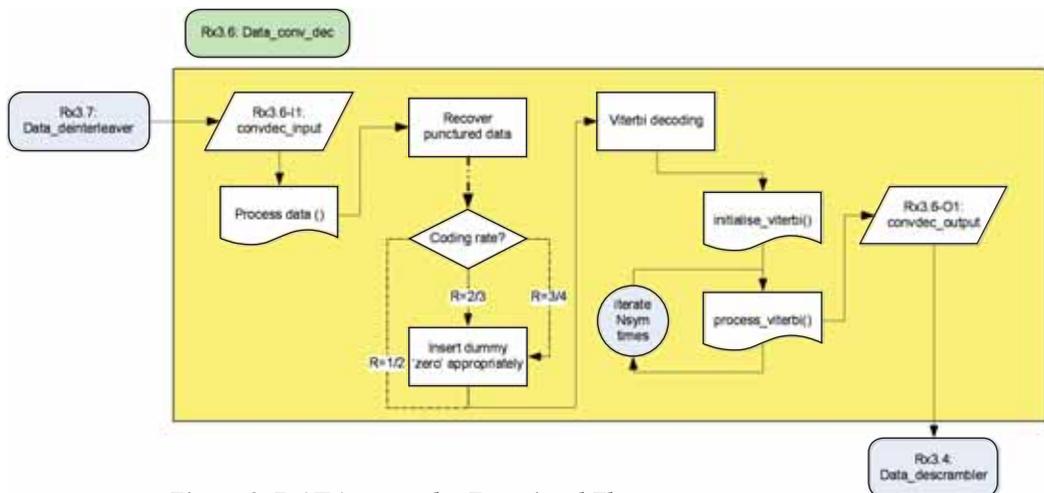


Figure 9. DATA_conv_dec Functional Flow.

dummy bits have to be inserted prior to the decoding. There is a fixed dummy bits insertion pattern to be followed for each coding rate. The complexity of the functional flow in *DATA_conv_dec* is shown in Figure 9. It is important to note that all these functionalities have been implemented using the open source OSSIE software and linked successfully with other components in the design.

Conclusion

Software defined radio has been the emerging trend of radio design both in the commercial and military arena. Wireless LAN standards like IEEE 802.11a have been among the popular physical means of data transmission. This thesis lays the groundwork for implementing an IEEE 802.11a standard using open source software for SDR design. Critical functionalities at the Physical layer have been implemented and the convenience and flexibilities of using software to implement a popular radio standard as compared to expensive and rigid radio implementation using hardware components demonstrated.

In this thesis, the author has successfully met the following objectives:

1. The IEEE 802.11a PHY layer transmitter has been built using a total of 23 OSSIE components with 12 different functionalities and 31 sequential I/O processes. Correspondingly, the receiver is implemented using 18 components with 12 different functionalities and 20 sequential I/O processes.

2. All these components have been designed with modularity and flexibility in mind so that they contribute to the pool of components for future radio design. Most of the functionalities reside in the *process_data()* functional call within the component C++ file for standardization and ease of debugging. “Read Me” files are also included in each component’s directory to explain its I/O data types, functionalities and assumptions. Appropriate parameters can be modified easily for use in other transceivers.

3. With the design implemented fully in OWD environment, the SDR conforms to SCA and CORBA. This will ensure flexibility, performance and maximum potential for software module reuse.

4. Using the test cases provided in Annex G of the IEEE 802.11a standard document, all the components have been verified to provide the necessary functionalities expected of them.

OSSIE, being the developmental software, has yet to release its full version. Most of the efforts from the OSSIE developers are channeled to fix bugs and enhance the software, rather than using the software to develop communications standards. This thesis leverages on the capabilities of the software, adapts it to a popular communication standard and advances OSSIE capabilities by demonstrating that such a marriage can be implemented with an integration of OSSIE components into a working waveform.

The Incremental Development Model was chosen for this thesis, and it comprises of three stages: Design, Develop and Verify. The advantage of this model is its incremental nature, which allows the developer to learn from earlier versions of the system and enhance the subsequent design. It provides a systematic approach of meeting the objectives of the thesis by adding verified components into the library and eventually forming the final product.

Recommendations

The software components developed here shall serve as a baseline to link up with other software or hardware components to implement a fully functional IEEE 802.11a transceiver. With the potential of implementing a fully functional radio standard, the follow up could be to use the developed components to test out the channel performances like Bit Error Rates (BER). Since the SDR is supposed to be modular and reconfigurable, its ability to be flexible in a dynamically changing environment can be further explored by changing parameters like the information bit rates in real time.

Academically, collaboration and research with Naval Postgraduate School and Virginia Tech can be enhanced with this family of components. The experiences and developments carried out in this thesis can also be exemplified for SDR education and training. 

Acknowledgements

The author would like to express his gratitude to Assistant Professor Frank Kragh and Professor R. Clark Robertson from the Naval Postgraduate School for their professional advice, guidance and assistance in making this thesis a possibility in such a short time. Their patience is greatly appreciated. The author is also grateful to the Republic of Singapore Air Force, for giving him this opportunity to study at the Naval Postgraduate School and carry out this interesting thesis work. This one-year experience has definitely enriched his knowledge in his professional and technical fields.

Endnotes

- ¹ J. H. Reed, *Software Radio: A Modern Approach to Radio Engineering* (New Jersey: Prentice Hall, 1st ed, 2002).
- ² IEEE Std 802.11a-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, high-speed physical layer in the 5 GHz Band" (Revision 2003).
- ³ Matthew S. Gast, "802.11 Wireless Networks – The Definitive Guide", Chapter 11: 802.11a – 5GHz OFDM PHY (O'Reilly, 2002).
- ⁴ Jacob A. DePriest, "A Practical Approach to Rapid Prototyping of SCA Waveforms" (Virginia Polytechnic Institute and State University, 2006).
- ⁵ "Definition of Iterative and Incremental development, Wikipedia." http://en.wikipedia.org/wiki/Iterative_and_incremental_development last accessed in Oct 2006.
- ⁶ Eric Christensen, Elisa Wing, "Waveform application development process for software defined radios", IEEE article, Motorola SSG and SPAWARSYSCEN (2000), p234.
- ⁷ Hiroshi Harada & Ramjee Prasad, "Simulation and software radio for mobile communications", Chapter 4: OFDM Transmission Technology (Boston: Artech House, 2002).
- ⁸ C. Britton Rorabaugh, *Simulating Wireless Communication Systems: Practical Models in C++* (New Jersey: Prentice Hall PTR, 2004).



MAJ Leong Wai Kiat, Chris, is currently a Project Manager in Air Plans Department. An Air Engineering Officer by training, he was formerly a Section Head in Air Logistics Department and an Officer-in-Charge in Air Logistics Squadron, Paya Lebar Air Base. MAJ Leong is a recipient of the SAF Local Study Award and the SAF Postgraduate Scholarship. He holds a Bachelor of Engineering (First Class Honours) in Electrical Engineering, a Master in Technology (Knowledge Engineering), and a Master of Science (Defence Technology and Systems) from the National University of Singapore, and a Master of Science (with Distinction) in Electrical Engineering from the US Naval Postgraduate School.

VIEWPOINT

Beyond Deterrence and Defence



Ruin in France during WWII; misperception and misperceptions are sources of deterrence failures.

Loe suggests that misperceptions might result from practical problems associated with intelligence and early warning processes. Failures in these processes might cause: (1) states not being able to act on warning signs even though there may be sufficient signs of an impending attack; (2) policy-makers to discount apparent threats as mere bluffs simply because they have become somewhat immune to such threats after prolonged periods of tension or because they have fallen prey to deception; and (3) problems of predictability arising out of ambiguity and ambivalence especially if the level of intelligence indicators remain low at the outbreak of crisis.¹⁴

Military Strategy and Deterrence

Others have postulated on the relationship between military strategy and the effectiveness of deterrence. According to Mearsheimer,

“conventional deterrence is directly related to how a nation’s armed forces are employed to achieve specific battlefield objectives”. He identified three principle strategies, each with a different implication on the effectiveness of deterrence. In general, when opposing forces are balanced, deterrence is very likely to succeed if the attacker is limited to attrition strategy as his only option or if the attacker is unable to force an early capitulation in the case of the limited aims strategy. On the other hand, deterrence is likely to fail if the attacker is able to employ a Blitzkrieg strategy. However, when the attacking side has overwhelming force superiority, Mearsheimer states that deterrence is very likely to fail regardless of the chosen strategy.¹⁵

Mearsheimer’s views were to a large extent substantiated by Rhodes. After surveying a host of empirical investigations on the effectiveness of conventional deterrence since the 1960s, Rhodes concluded that deterrence could succeed if potential aggressors were denied a quick military victory and political gain.¹⁶

Nevertheless, an opposite argument to Mearsheimer’s postulation might also be true. There is every possibility that an attacker would be able to “design around” conventional military deterrence through if information about the deterrer’s defence strategies are available.¹⁷

The Interconnectivity of Military and Political Considerations

Deterrence strategy refers to the application of deterrence theory to real world conflicts, and the purpose of

In his article, “Is the Concept of Deterrence as a Key Survival Strategy for Small States Fundamentally Flawed?”, MAJ Harold Sim correctly pointed out that there are situations where a potential enemy cannot be deterred at all. Despite the unreliability of deterrence, it remains a useful strategy and could be made more successful when coupled with diplomacy.

When both deterrence and diplomacy fail, an oft-stated recourse is defence – the use of force to fend off an attack. Beyond these, this Viewpoint would

also like to briefly touch on the other options of pre-emption, compellence and offence.

Before we discuss further, it is relevant to further explore the shortcomings of deterrence. One area of deterrence failure occurs in a preventive war situation. In this scenario, a declining state relative to a rising state prefers war over peace. Regardless of the forces arrayed against it, the declining state will initiate hostilities, sooner rather than later, because its strength relative to its opponent’s grows weaker as time

goes on. The greater potential of the rising state is cause to strike now.

The Japanese initiation of the Pacific War is a classic example of preventive war. American aerial deterrence in the Philippines in the form of B-17 strategic bombers and British naval deterrence with Force Z both failed because the Japanese proved undeterrable. It was better to attack the United States now while it has yet to achieve its full war potential and take advantage of British weakness in the Far East to occupy its resource rich colonies. The military capabilities represented by both the aerial and naval deterrence was too weak and hence not credible. Allied deterrence could be neutralised by highly trained land-based Japanese air forces using long-range aerial interdiction from bases in French Indochina and Formosa.¹

In a preventive war situation then, since deterrence has failed, one possible recourse is pre-emption – the mounting of a spoiling attack to disrupt the expected enemy offensive. In other words, an offensive defence. But this assumes that the defending state possesses a strategic culture that embraces the use of pre-emption. The moral high ground adopted by the Western democracies during the Second World War made pre-emption an undesirable option despite the profusion of pre-emptive operational plans. Neither do democracies violate the neutrality of neutral states. Nor do they deliver the first blow in the face of enemy provocation. Both the British and American theatre commanders refused to strike the first blow, preferring that the Japanese made the first overt move.

This reluctance sharply compromised the Allied defence of their colonial possessions. While pre-emption could be an option, the relative merits accruing to a small state (in a weak geopolitical position and with relatively fewer resources to mobilise) to deliver rather than absorb the first blow or even to simultaneously exchange blows with its opponent remains debatable.

When deterrence is not reliable and pre-emption is problematic, what other strategies are we left with? Compellence – seeking to coerce an opposing state and bend it to your will by forcing it to do your bidding against its wishes – has become a more attractive and viable option if the small state possesses credible military capabilities. Compellence, which may involve the use of force or the mere demonstration of force, may prove to be a more useful military strategy in pursuit of a political objective. It necessarily requires the flexing of military muscles, and is an inherently assertive, if not aggressive, strategy. Force may or may not be used. In the former, any war involves the use of compellence, using force to make the target state yield to your demands. In the latter, this involves the demonstration of force to achieve a state’s political objective. Compellence is conceptually different from deterrence. Compellence “seeks to compel an adversary state to actually do something it would otherwise not do” whereas deterrence makes an adversary state “refrain from doing something it would like to do”.²

Finally, to round off this discussion, the concept of offence must be raised. This refers to the launching of attacks

on other states to secure political objectives. In other words, using force to achieve national goals. To the layman, it is inconceivable for small states to resort to offence as a grand strategy. But history is replete with examples of small states that used offence successfully. Macedonia, Prussia and Manchuria were small, weak states on the fringes of large, powerful neighbours. But their successful use of offence transformed them into either great empires or great powers. In our current world though, international laws and norms heavily circumscribe the use of force. The price

of violating another state's sovereignty is extremely high and makes any use of offence a daunting prospect. This fact should allow readers to sleep easier at night. 🙏

*Mr Toh Boon Kwan
(NSman, SAFTI MI)*

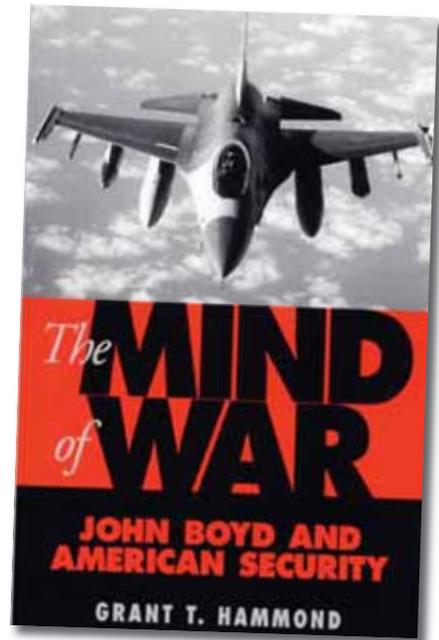
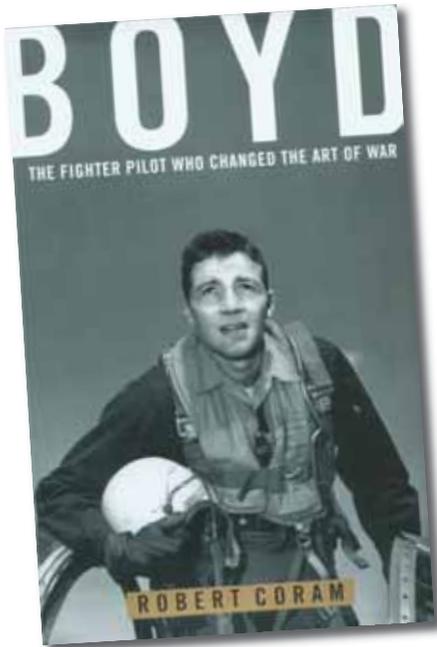
Endnotes

- ¹ Japanese responses to American and British deterrence are detailed in William H. Bartsch, *December 8, 1941: MacArthur's Pearl Harbor* (College Station: Texas A&M University Press, 2003), pp191-192, p232.
- ² The definitions of compellence and deterrence are cited in Philip Bobbitt, *The Shield of Achilles: War, Peace and the Course of History* (London: Penguin Books, 2003), p13.

BOOK REVIEW

Colonel John Boyd – The Man, His Contributions and Some Reflections for ‘Personnel’ Transformation

by CPT Phua Chao Rong, Charles



Coram, R., *Boyd: The Fighter Pilot who changed the Art of War* (New York: Back Bay Books, 2002).

Hammond, G. T., *The Mind of War: John Boyd and American Security* (Washington: Smithsonian Books, 2001).

John Boyd was a first-rate fighter pilot, engineer and scholar. The intellectual leader of the US Military Reform Movement, he sacrificed his career (‘retired’ as Colonel) for his beliefs and theories on manoeuvrability, Manoeuvre Warfare and OODA loop (Observe, Orient, Decide and Act),

which have truly passed the test of time. His arduous journey to accomplish these provides fruitful reflections for the SAF’s current transformational efforts.

Both books differ in their approaches. Coram’s thick biography is filled with anecdotes of Boyd’s growth,

family and friends using extended sources provided by Boyd's friends – an engaging read by an author who was twice nominated for the Pulitzer Prize. In contrast, Professor Hammond at the Air War College presents an academically rigorous examination of the core of Boyd's thinking and its implications on US security.

Boyd was famous for his creativity, and infamous for his stubborn advances against the bureaucratic conformist system in order to advance his personal beliefs of 'what is right'. Boyd was motivated by competition, self-perfection and progress rather than fame. Boyd was arguably the greatest fighter pilot in American history. As an instructor, he defeated every pilot who challenged him, in less than forty seconds, to gain the accolade – Forty Seconds Boyd. He strived in competition but he contributed back with his 150-page manual 'Aerial Attack Study', which eventually became the official tactics manual for fighter pilots.

The quest for self-perfection propelled Boyd to take up a second degree in Industrial Engineering, which gave him the tools to unravel his next big discovery – the Energy Manoeuvrability (EM) theory. Armed with empirical evidence, he fought hard to re-design the F-15 from an 80,000-pound, swing-wing behemoth to a 40,000-pound fixed wing-manoeuving fighter, but with limited success. In a second counter-attack, Boyd finally pushed his ideas through into the F-16 and this remains one of the most manoeuvrable fighters ever designed. Through the process of fighting, this warrior-scientist also received the nickname of 'Mad Major'

for being so mission-oriented, to the extent of 'burning a hole in a general's tie' who actually agreed with him.

However, Boyd's greatest contribution was to expound on Sun Tzu's ideas within the US military and ensured that the US military progressed in its strategic thought as much as it has in the technological field. An avid reader of military history and strategy, Boyd was deeply influenced by Sun Tzu amongst other military theorists and practitioners. He owned seven translations of the 'Art of War', which is the only military classic that Boyd did not have qualms about. The product is the OODA loop which is 'an updated and elaborated, albeit unintended, reinterpretation of Sun Tzu'. It consistently used 'Sun Tzu's ideas to overcome Clausewitz's overemphasis on achieving decisive battles by overcoming friction and the underemphasis on strategic manoeuvre'. That is why Berkowitz declared Boyd to be the American Sun Tzu.

His influence within the US military was far-reaching. Boyd did so via his legendary 6 to 8-hour briefings on 'Patterns of Conflict', delivered over 1,500 times, and where he would introduce ideas of Sun Tzu and its applications in battles of Napoleon and Genghis Khan. Boyd was uncompromising on the length of the briefing but 6 to 8 hours was exactly the time he needed to convince most of his audience of his and Sun Tzu's ideas. His audiences in the 1980s and 1990s included former Secretary of Defense and current Vice President Dick Cheney, Sam Nunn (former Chairman of the Senate Armed Services Committee), Newt Gingrich (former Speaker of the

House whose 7-point plan on the Long War was circulated to the Joint Chiefs of Staff by Donald Rumsfeld on 30 Jan 06), General Al Gray [former Commandant, US Marine Corps (USMC)], and General Edward Myer (former Chief of Staff of the US Army).

In fact, there is evidence to believe that it was precisely Sun Tzu/Boyd's manoeuvre warfare that enabled the US to win Operation Desert Storm. Boyd had a direct role in its strategic planning. According to Coram, then Secretary of Defense Cheney invited Boyd to the Pentagon to discuss the strategic aspects. With Boyd as his background advisor and the support of Colin Powell (then-Chairman, Joint Chiefs of Staff), Cheney rejected General Schwarzkopf's initial plan for a head-to-head assault against the main Iraqi forces (classic attrition warfare) in favour of a left-hook manoeuvre led by the Marines. The result was 'a first rate instance of Sun Tzu's cheng/chi' and the surrender of 15 Iraqi divisions to 2 Marine divisions. After the victory, the US military spokesperson's words were 'we kind of got inside his decision [Boyd's OODA] cycle'. As General Krulak, Commandant of the USMC testified, 'Boyd was the architect of that victory'.

However, the influence of Boyd was uneven across the Services. The process was gradual and was facilitated by his associates (Acolytes) whom he insisted that they read and reread Sun Tzu. The Marines were most friendly to Boyd probably due to his relationships with Colonel Wyly (retired Vice President of USMC University) and former Commandant, General Al Gray. Boyd

lectured several times a year at the Marine Basic School and thus trained a generation of Marines on Sun Tzu. Sun Tzu/Boyd's manoeuvre warfare can be found in FMFM-1, the USMC 'Warfighting' manual, which was conceived by General Gray who further instructed all Marines 'to read and reread' it. Gray and Captain Schmidt (drafter) later insisted that it was inspired by Sun Tzu (and hence Boyd) rather than Clausewitz. The US Army was less receptive to Boyd's ideas. Boyd only lectured at the Army War College and Fort Leavenworth a few times due to the influence of Huba Wass de Czege (his Acolytes). In addition, the US Air Force least welcomed Boyd, albeit him lecturing at the Air War College for a short while. He also spoke a few times to the US Navy in Florida.

Nevertheless, Boyd's contributions and breakthroughs were substantial and were the results of years of hard work fighting against the civilian and military bureaucracy. Boyd struggled as the creator, chief strategist and spiritual leader of the Military Reform Movement, otherwise known as 'Genghis John'. Boyd had a choice – to be or to do? He can opt to be somebody – by keeping quiet on reforms and ride on his 'Forty Seconds Boyd' tactical flight success. However, Boyd chose the tougher road – to do important things and make a real contribution to society even if it was at the expense of career advancement. In the end, the US military still benefited from Boyd's EM theory, F-16s, OODA loop and Manoeuvre Warfare albeit with a considerable amount of havoc. Like his philosophy on manoeuvre warfare, Boyd had to manoeuvre his way through to effect change. He fought

amazing battles against the Pentagon using media such as Time magazine over the Pentagon's overspending, and got Congress into a two-year debate over the Army's Bradley Fighting Vehicle using The Washington Post and The New York Times. His intention was clearly to highlight the potential business interests and/or conspiracies behind some defence projects. His methods may be unorthodox and impolite but his conscience was clear; he was right and he won.

It is interesting to note the fate of the military mavericks like Boyd. Despite his many ground-breaking contributions to the US military, Boyd was never really given due recognition. To an extent, then-British Prime Minister David Lloyd George's statement on Colonel Richard Meinertzhagen (WWI) still seem to ring true today across the militaries in the world: 'One of the most able and successful brains I met in any army. Needless to say, he never rose in the war above the rank of colonel.' The same can be said of strategists like Colonel T.E. Lawrence and Captain Liddell Hart in the UK. In the contemporary US military, Boyd is an example of a sidelined maverick; his associates, like Colonel Wyly, were forced into early retirement, because Boyd testified at a Congressional hearing that 'the Marine Corps still had senior officers with an old attrition-war mindset'. Boyd's final advice to the Congress in 1991 was that if nothing was changed, "it would inhibit young Marine officers from proposing crucial new ideas and the Marine Corps would be ruled by 'dinosaurs'". Is the military bureaucracy inevitably bound by Manichean politics (either blend

into the specific strategic culture or 'get out')?

These are interesting observations and important questions for the SAF to ponder as it embarks upon its own transformation where change and creativity is not only necessary but also crucial. Perhaps Boyd has his own competitive attitude and aggressive personality to blame for not rising beyond the rank of Colonel. However, it might precisely be this personality that flourishes creativity and drives change. His contributions are far-reaching but his career advancement does not correspond with his legacy. This disparity between an individual officer's milestones and his/her career advancement will be a key issue militaries undergoing transformation will have to encounter and address.

The *POINTER* monograph on leadership suggests a Route of Contribution (ROC)-centric over a Route of Advancement (ROA)-centric culture. From this, a contribution-based criterion for military personnel's 'route of advancement' could be inferred and this plausible solution ensures that Boyd's career advancement will be assessed based on his contribution to the overall well-being of the US military and its transformation journey. In Singapore, civil-military relations, defence diplomacy, technological innovation and strategic aspects of war have taken on a new significance. The contribution-based criterion thus assesses the peacetime civil servant/scholar/diplomat-soldier, while the present performance assessment criteria rightly assesses the operational

readiness/capabilities of the wartime warrior-soldier. With a triangulation of both criteria, therein lies the possibility of grooming future John Boyds for the SAF.

Besides, one also observes that creativity is his part-time job done at home, in the evenings and early mornings. One questions if Boyd might be as creative if he was in a full time Defense Advanced Research Project Agency job. Boyd reads a lot and his creativity comes in sparks. Based on this, perhaps the Future Systems Directorate (FSD) and SAF Centre for Military Experimentation might consider providing an environment for non-FSD officers to embark upon military experimentation and test ideas for transformation on a part-time/project basis. This potentially opens up the Pandora's box for military security and human resources; however, the contribution-based approach seems to simplify the latter problem at least [i.e. one is assessed based on his routine job (operational readiness) and also on his additional contributions to the SAF (military experimentation and any

other contributions that benefits the organisation)].

In conclusion, based on Boyd's contributions, there is little wonder why he was the first Air Force pilot to be bestowed the Marine Corp insignia during burial – the highest honour a Marine can receive. Although he deserved more in his career, his contributions to the military are beyond what the highest honour can tangibly reflect. Boyd's life shows that everything is possible with hard work. Boyd had an IQ of only 90 but he got two degrees in Economics and Industrial Engineering. More importantly, his contributions to the US military and even the business community are more significant than many others who have higher qualifications or IQ. This is the power of self-motivation, the right attitude towards learning and the effect of constant reading. Both books adequately offer fruitful insights into these aspects of Boyd's life and his contributions to the US transformation. Therefore, they remain useful sources of reflection for the SAF's own transformation journey. 



CPT Phua Chao Rong, Charles, is currently a Platoon Commander in HQ Armour. An Intelligence Officer by training, CPT Phua is a recipient of the Academic Training Award (Overseas) and he holds a Bachelor of Science (Second Class Upper Honours) in International Relations and a Master of Science (Research) with Merit in International Relations from London School of Economics (LSE), U.K. CPT Phua is also the recipient of the Goldman Sachs Global Leader Award (2004) for academic and leadership excellence at LSE and the 2005 HSBC Youth Excellence Award for youth leadership and community service.

FEATURED AUTHORS

Robert Coram and Grant T. Hammond



Robert Coram

Robert Coram's breadth of expertise and interest is nothing short of astounding. Kicking off his career as a reporter for *The Atlanta Journal* when he was a sophomore in college, he was a general assignment reporter but he also wrote features, book reviews, travel stories, and aviation stories. He notably covered the civil rights movement in Atlanta during the 1960s. Shortly after, he began to write freelance articles; first for the then-new *Atlanta Magazine*, then for aviation publications and national



magazines. Easily one of the more versatile authors that most people will ever come across, Coram's accolades and achievements span three decades, testament to his legacy not only in the military and academic circles, but also in categories like fiction and human interest stories.

In 1976, Coram broke new ground by writing the first piece about narcotics trafficking in a national magazine. In the late 1970s, he travelled extensively in Colombia, Jamaica, the Turks & Caicos Islands, the Bahamas and south Florida,

researching and immersing himself into the seedy world of drug trafficking, eventually producing articles so mesmerizing, he was asked to become a reporter for *The Atlanta Constitution*. The first year as a reporter, he received a Pulitzer Prize nomination for his stories about drug smuggling. By his second year at *The Atlanta Constitution* he was covering the war in El Salvador. He received another Pulitzer Prize nomination for a series of articles that stopped the National Park Service from developing Cumberland Island. Coram is the epitome of a writer whose works strike a chord deep in the core of his readers – he composes articles that many can relate to and identify with.

An avid fiction writer, Coram is also the man behind titles such as *Kill the Angels* and *Atlanta Heat*. By the end of the 1990s, Coram decided to revisit his non-fiction roots, starting on the biography of John Boyd, a project that took almost three years to complete. Little did he know that he was about to create a biography so moving and powerful that Senator Charles Grassley proclaimed, “Coram has captured the invincible spirit that is John Boyd in all its fury and intensity of purpose and genius”. William Diehl, the author of *Eureka*, was also quoted as saying “What a story... Coram tells this unforgettable story with the same passion as the man who lived it.” Indeed, *Boyd: The Fighter Pilot Who Changed the Art of War* is as authoritative and riveting as a biography can get.

In an exclusive interview with management consulting and leadership and training development firm Tompeters.com, Coram said when

he was conversing with a few “Boyd Acolytes”, he “realized that this (the story of John Boyd) was probably the best story I had ever run across”. He then proceeded to write a 65-page proposal by week’s end and by the following Monday afternoon, the prototype was sold to Little, Brown and Company. When faced with a story that he is so deeply passionate about, Coram was able to translate his fire for Boyd’s amazing life into what is frankly, an astonishingly captivating publication. Perhaps the most poignant quote from the interview was Coram boldly proclaiming that Boyd “was one of those people who just put the bit in his teeth and did what he thought was right and devil take the hindmost”. He was keen to be adventurous, take chances, and accept the outcomes of his actions. Echoes of Boyd’s philosophy of living life can be seen in Coram’s own; he was audacious, daring and always allowed passion and verve to lead the way. Coram also had an intimate association with the military. He often told people that he never had a childhood, but “had a rather extended boot camp”. Coram’s father was a top sergeant in the US Army and spent thirty-three years in the organisation. In writing Boyd, he came to realise new things about military culture and history that “make them better than the rest of us”. Coram’s rationale was that the military has a higher sense of honour, code of standards, and patriotism, and that people in the military have a contract that goes up to including the loss of life, and their level of dedication to the country is second to none. It is hence unfortunate that “civilians don’t have

that kind of contract”, thus the need to cherish the commitment of militaries even more than we do now.



Grant T. Hammond

Dr Grant T. Hammond has been Director of the Centre for Strategy and Technology (CSAT) and Professor of Strategy and International Security at the Air War College since 1989. His publications include *Countertrade, Offsets and Barter in International Political Economy*; *Plowshares Into Swords: Arms Races in International Politics, 1840-1991* and *The Mind of War: John Boyd and American Security*. Testament to his treasure cove of experience and knowledge, Hammond’s works has been published in a series of prestigious journals including *Air and Space Power Journal*, *Defence and Security Analysis*, *Joint Force Quarterly*, *The Journal of Conflict Studies*, *Washington Quarterly*, *Small Wars and Insurgencies*, and the *Journal of Innovation and Management*, among others.

Hammond is a regular guest lecturer on defence issues both in his country of origin and abroad, and he speaks on a diverse range of issues including future conflict, creative thinking, strategy and airpower. Hammond holds a Bachelor of Arts from Harvard University and a Master of Arts and PhD in International Relations from the School of Advanced International Studies of Johns Hopkins University. Hammond has written extensively on arms transfers, the militarization of

space, low intensity conflict, American foreign policy, among others. Hammond served as the executive officer of the Centre of International Affairs at Harvard University before joining the faculty at the Air War College. His leading areas of research and interests are the strategic and technological choices, challenges and outcomes of confronting the US and the nature of emerging conflict. Hammond will be leaving the Air War College in the Fall of 2007 to become Dean of the NATO Defence College in Rome.

One of Hammond’s most provocative works is *Plowshares Into Swords: Arms Races in International Politics, 1840-1991*, where he explores the phenomenon of the arms race, a subject of vital significance to the international community for the past century and a half. In this comprehensive overview, Hammond succinctly defines the characteristics of arms races, evaluates their catalysts and triggers, lucidly describes how arms races were conducted, and their overall impact on global politics. Typical of Hammond’s inspired delivery, he does not limit his discussion to merely that of the international arena but artfully places emphasis on the consequence of arsenal-building competition on a country’s local affairs as well. Perhaps the critical ingredient that makes *Plowshares Into Swords* such an intriguing chef-d’oeuvre is Hammond’s underlying ability to blend historical references and analysis with political and economic lessons, which he then drizzles with illuminating examples. The result is “not only a vivid description but also a clear explanation of the phenomenon that has both been blamed for the instigation of war and heralded for its prevention”.

In *The Mind of War: John Boyd and American Security*, Hammond crafts a compelling account of a man who had a tremendous impact not only on the military, but American thought. Like Boyd, Hammond as an author “was never static. He kept moving, kept developing and expanding”, eventually becoming the accomplished author he is today. Hammond mentioned in *The Mind of War* that Boyd was greatly influenced by Sun Tzu and other military theorists, and that he sought to translate ideas into action. Parallels can easily be drawn between the subject and the author; Hammond’s howling masterpiece is the embodiment of an individual with great integrity and morality. Perhaps in the future, prominent military figures will be looking for inspiration from Hammond’s works, if it is not already happening. What sets Hammond’s *The Mind of War* apart from other John Boyd pieces is his unfailingly precise and rigorous investigation of the root of Boyd’s motivations and ultimately, its significance on US military policy. Although the book’s readership may be limited to individuals seeking in depth knowledge of John Boyd, it keenly rewards the avid reader, providing in spades historical knowledge and relevant analysis that transcend trends and the barriers of time. Few other authors have come close to achieving

Hammond’s level of dedication and commitment to his craft and expertise; surely, his illustrious career at the Air War College has shaped the brilliant academic and author that Hammond is today.



Both Coram and Hammond are extraordinarily accomplished writers in their own right; each taking a vastly different approach to military and strategic issues. It is with contrast do we truly appreciate the strengths of these authors, and, when their styles and thoughts converge into two powerful publications, namely *The Mind of War: John Boyd and American Security* and *Boyd: The Fighter Pilot Who Changed the Art of War*, we as readers are thrown into a new dimension of celebrating John Boyd for both his inspirational story and his contributions to the military and American thought. As aptly described by Coram, Boyd was “the sort of man that all of us admire, and I think many of us secretly aspire to be”. Certainly, the wealth of knowledge and strategic lessons that Coram and Hammond have enriched the academic world with is, in itself, worthy of admiration. *POINTER* is honoured to feature the works of these brilliant authors. 🇺🇸

PERSONALITY PROFILE

General Sudirman

Introduction

General Sudirman (24 Jan 1919 – 29 Jan 1950) remains one of Indonesia's most revered national heroes today. As the first Commander-in-Chief of the Indonesian armed forces, he united and led the Indonesian forces in resisting colonial re-occupation after the Japanese Occupation. His leadership style and personal ideals about the Indonesian military as the steadfast defender of the Indonesian nation laid the foundation of the Indonesian military system.

Early Life

Sudirman was born into a poor family in Rembang in western Central Java. His uncle, a civil servant, adopted him as his son and provided him an education. He studied at the Dutch Native School in Purwokerto but later transferred to a nationalist school, where he became strongly influenced by nationalism and Islam. While studying, he joined a boy scouts group of Muhammadiyah, a reformist Moslem organization and eventually became a teacher at a Muhammadiyah secondary school in Cilacap and a leader of the organization's youth wing. Clearly, his education and activities during his youth had fuelled his patriotism, nationalism and religiosity and also



developed his leadership ability. He did not display the usual martial qualities of a heroic military leader; instead, he was a soft-spoken and devout Moslem but extremely charismatic, strong-willed and firm.

Rise to Prominence: The Japanese Occupation and After

After the Japanese successfully invaded Dutch-controlled Indonesia, they recruited and trained Indonesian pemuda (youths) to form an auxiliary

military force known as PETA [Pembela Tanah Air]. The Japanese selected prominent locals to lead these units and Sudirman was unsurprisingly selected to be one such daidanchō (battalion commander). When the Japanese surrender became inevitable in 1945, Sukarno and Mohammad Hatta declared Indonesia's independence on 17 Aug. The Indonesian army, the TKR (Tentera Keselamatan Rakyat – the People's Security Army) was formed on 5 Oct out of self-formed local units, mostly constituted by ex-PETA members who had been disbanded by the Japanese to prepare for Allied reoccupation.¹ Instead of disbanding, Sudirman kept his Banyamus-based regiment together and he scored a major accomplishment by persuading the Japanese to turn their weapons over to them. This resulted in the procurement of a huge arms cache, more than sufficient for his own unit, and he distributed the remainder to other Javanese groups, winning their support. Consequently, while other PETA units dispersed, his unit became the best armed and the best organized.

The opportunity for Sudirman to demonstrate his faculties for military command arrived soon. Tensions escalated after British forces landed in Indonesia to supervise the Japanese surrender and preserve order, which eventually culminated in the outbreak of violence between the British and the Indonesian independence fighters. Negotiations for a ceasefire broke down and more Allied troops arrived. By late November, the British and Dutch troops had withdrawn to Ambarawa

to form a strong defensive ring, the destruction of which required a consolidated and unified command. Consequently, Sudirman gathered and organized all commanders in the sector for a coordinated attack, which astoundingly routed the Allied forces on 15 Dec. A month earlier, on 12 Nov, he had already been elected by the other Indonesian military commanders as the Commander-in-Chief (panglima besar) of all Indonesian forces. Three days after the resounding victory at Ambarawa, his appointment was formally inaugurated by President Sukarno; he was only 29 years old then.

Securing Independence: The War against the Dutch

The British were soon replaced by the Dutch with whom negotiations continued throughout 1946-1948 amidst mutual distrust and continued tensions. Eventually despairing at the probability of a diplomatic solution, the Dutch sprang a rapid invasion, with bombers bombing Manguwo, Yogyakarta's airport and paratroops dropped near and into the capital. Sudirman hastened to see Sukarno immediately, despite being gravely stricken with tuberculosis. He had anticipated the inevitability of a Dutch attack and retained day-to-day command of the army. At the Presidential Palace, he refused to obey Sukarno's pleas for him to return home to rest. Furthermore, he rejected Sukarno and Vice-President Hatta's decision to remain and let themselves be captured. When he was convinced that the civilian leaders were adamant

on surrender, he left the city after issuing Emergency Order No. 1.PB/D/48, ordering the entire Indonesian military to abandon linear defense and retreat to the non-urban areas to wage a guerilla war. Even before the invasion, Sudirman and his commanders had begun to prepare for a guerilla war, to exploit Indonesia's terrain and geography and the Indonesians' superior spirit and morale against the enemy's sophisticated weaponry.

Sudirman retreated into the jungle under hot pursuit by the Dutch, who were eager to distribute erroneous propaganda emphasizing his capture, demonstrating their acknowledgement of his influence.² Naturally, the news that Sudirman was not caught and was in fact leading the resistance reverberated throughout Indonesia and the Dutch consequently sought him relentlessly, attacking and intensifying patrols in areas he was believed to be traversing. Thus, Sudirman's feat of achieving independence for Indonesia was even more redoubtable; he made an arduous journey under Dutch pressure in deteriorating health and with minimal resources. He had to be carried on a sedan chair throughout the journey, which saw him traveling as far as 1,000 kilometers for six months before settling down at Sobo on 1 Apr 1949, all while continuing to lead the guerilla war against the Dutch.

Crucially, he understood the necessity of galvanizing and utilizing the people's support in war and this warranted the decision to rely on guerilla warfare instead of committing the military alone in a conventional defense. Furthermore,

the political turmoil in Indonesia led to weak governmental guidance and control and the civilian surrender in the face of the Dutch aggression induced the military to take it upon itself to take over the government for eight months. To Sudirman, 'what is important is that we win the war, not the battles'; in embracing guerilla warfare, Sudirman was utilizing the means he possessed in the best way to achieve the desired political ends.³ Prior to the urgent order to launch guerilla war, Colonel A.H. Nasution had already formulated a grand strategy which involved the abandonment of linear defenses for guerilla tactics and a scorched earth policy, with the formation of self-sufficient cells in each district to extend the war across Java. Thus, the Dutch was unable to destroy the Indonesian army fighting with the support of the Indonesian people, undermining Dutch justifications for re-occupying Indonesia. Instead, Dutch troop morale became dampened by the extension of the conflict as they hunted for the TNI which harassed the Dutch forces and positions incessantly. Sudirman judged correctly that the Dutch would be unable to sustain the invasion as international and Dutch domestic criticisms were provoked by a costly protracted engagement fought to preserve a colonial empire.

Negotiations between the Dutch and Indonesian civilian leaders began in April 1949, culminating in the Rum-Royen Agreement of May 7 which called for a ceasefire by the guerilla fighters and a roundtable conference as a step towards the unconditional transfer of sovereignty to Indonesia.

Given the authority Sudirman wielded, Sukarno quickly sent Lieutenant-Colonel Suharto to deliver a letter written by the ruler of Yogyakarta to persuade Sudirman to return to the capital. However, despite the moving reunion meeting between Indonesia's civilian leaders and its top military commander in Yogyakarta on 10 Jul 1949, Sudirman quickly denounced the agreement. Fearing a repeat of the 1948 situation where diplomacy only gifted the Dutch time to consolidate their forces, he refused to relent, preferring a ceasefire only after a satisfactorily-concluded negotiation, and asked to resign together with Colonel Nasution if the government insisted on accepting the agreement. Sukarno's response was to declare that 'if the leaders of TNI resign because of this, we as the president and the supreme commander will also resign'.⁴ Eventually, Sudirman, under Nasution's counsel, abandoned his threat of resignation and accepted the government's stance. The ceasefire took effect throughout Java on 11 Aug and in Sumatra four days later. On 27 Dec 1949, the Dutch formally transferred sovereignty to the state which eventually became the Republic of Indonesia on 15 Aug 1950.

Patriot and Unifier

Sudirman's greatest legacy was his unwavering selfless patriotism, prioritizing the nation's security and sovereignty above his life. In a formal investiture on 25 May 1946, Sudirman represented himself and his subordinates in uttering the Members of the Forces leadership oath, first and foremost swearing to:

"...Ablly defend the sovereignty and independence of the state of the Republic of Indonesia that was declared on 17 August 1945 to the last drop of blood."⁵

He quickly sought to instill in his armed forces the vision of the Indonesian army he aspired, instructing that:

"Soldiers have only one obligation, to defend the sovereignty of the state and ensure its safety....Obey your superiors and carry out all responsibilities to the best of your ability..."⁶

His very personal style of leadership and the challenges he confronted were physically and mentally draining, which exacerbated his ill-health, but he did not relinquish his duties and responsibilities. The grueling flight from Yogyakarta while continuing to direct the resistance war he endured testified to his resolve and dedication as Commander-in-Chief of his nation's defenders. He finally succumbed to his condition only a month after Indonesia formally attained its independence, symbolically vindicating his oath to defend his nation to his last breath, dying at a young age of 31.

Sudirman's prioritization of the country's independence over everything else made him prefer the preservation of the military's autonomy from the civilian government. In the years after his installation as Commander-in-Chief, factionalism among the Indonesian politicians continued. Amid the politicking, Sudirman remained aloof, not taking any sides while continuing

to protect the unity and integrity of Indonesia, although he inevitably became the target of slander. While he attempted to mediate between the quarrelling factions, he disassociated the military from the politicians, whom he felt were more interested in their narrow political interests than the freedom of the country, to avoid the military's ability and motivation to mobilize and fight being affected. His strong beliefs about the mission and position of the TNI became a legacy of Indonesia's brand of civil-military relations, where the military viewed itself as the paramount protector of Indonesia's sovereignty and security.

As Commander-in-Chief, his most important role was in unifying the disparate rival Indonesian armed groups that formed following the Japanese defeat into a coherent structured military organization. The greatest hostility was between the Japanese-trained ex-PETA members and the Dutch-educated Indonesian soldiers who had served in the Royal Netherlands Indies Army (KNIL); they were constantly suspicious of each other. Even within KNIL, there was antagonism between the senior officers, and the younger officers who sought to supplant them. Hence, there was the need for the special military conference attended by all the commanders of military units from Java and Sumatra held on 11 Nov 1945 in Yogyakarta. That Sudirman was elected was a clear sign of the support and trust he commanded. Despite being only slightly older than most of his soldiers and officers, he behaved like a father figure to the armed forces, who

addressed him as Pak Dirman out of reverence and respect. He pursued an open, accommodating style of leadership and solicited advice from anybody he met, including his opponents, and endeavoured to listen to all perspectives and viewpoints before making a firm decision. This was partly because he recognized his own inadequacies, and partly because he saw the importance of maintaining good relations with all centers of power and of maintaining harmony within the army. For example, after being elected as Commander-in-Chief, he immediately retained as Chief-of Staff Urip Sumoharjo, the well-trained and experienced commander of the KNIL, and entrusted to him the military aspects of commanding the Indonesian army, despite his unpopularity with Sudirman's ex-PETA counterparts. Similarly, recognizing Nasution's capabilities and experience in conducting guerilla warfare since the first Dutch attack in 1947, he unhesitatingly allowed Nasution free rein in implementing his concept of total guerilla warfare, despite the Dutch-trained officer often opposing Sudirman on other matters.

Conclusion

Sudirman died in Magelang on 29 Jan 1950, leaving a wife, seven children and a nation in bereavement. In recognition of his achievements, he was buried in the – Heroes' Cemetery in Semaki, Yogyakarta and pronounced a National Hero of Indonesia (Pahlawan Pembela Kemerdekaan – Independence Defender Hero). During a tumultuous era, Sudirman unified a disorganized but nationalistic collection of armed groups

into a military organization capable of defeating a technologically superior enemy. His selfless patriotism and personal charm gained the trust of his President, respect from the Indonesian people, and his subordinates' loyalty – 'a symbol of exalted service to his nation and his people which would be difficult for anyone to match'.⁷ Today, Indonesia remembers Sudirman in many ways, including the naming of major streets in Indonesian cities and the University of Jeneral Soedirman in Purwokerto after him. Numerous statues, memorials and a museum are dedicated to commemorating his contributions. Most symbolically, a tall statue of Sudirman was erected before the Indonesian military headquarters

in Cilangkap in 1991, cementing his historic place as the Father of the Indonesian armed forces. ©

Endnotes

- ¹ TKR became the TRI (Indonesian Republic Force) in January 1946 and later, the ABRI (Angkatan Bersenjata Republic Indonesia – Armed Forces of the Republic of Indonesia). Today, the Indonesian military is known as the TNI (Tentara Nasional Indonesia – Indonesian National Army).
- ² Tjokropranolo (Lieutenant General, Ret.), *General Sudirman: The Leader Who Finally Destroyed Colonialism in Indonesia*. Translated by Libby Krahling, Bert Jordan & Steve Dawson; edited by Ian MacFarling (Canberra, A.C.T.: Australian Defence Studies Centre, 1995), p107.
- ³ *Ibid.*, pp157-158.
- ⁴ Salim Said, *Genesis of Power: General Sudirman and the Indonesian Military in Politics, 1945-49* (Singapore: Institute of Southeast Asian Studies, 1991), p121.
- ⁵ Tjokropranolo, *General Sudirman*, p54.
- ⁶ *Ibid.*
- ⁷ *Ibid.*, p153.



CDF Essay Competition 2007

POINTER is pleased to announce the
21st Annual Chief of Defence Force Essay Competition.

The CDF Essay Competition aims to encourage SAF Officers to **conduct research** on professional and military-related issues relevant to the SAF. You are invited to **share your knowledge, ideas and reflections** on Warfighting/Force Transformation, Leadership/Organisational Development, or Conflict & Security Studies. All entries must be submitted in soft copy and be accompanied by a soft copy entry form. The form can be downloaded at the *POINTER* website @ <http://www.mindef.gov.sg/safti/pointer>

All Regular/Full-time National Service/National Service Officers, Officer Cadets, Warrant Officers, Defence Executive Officers and Defence, Science & Technology Agency personnel are welcome to participate.

Submit your entry early. The CDF Essay Competition 2007 is closing on 31 Dec 07.

