POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

Vol. 42 No. 3 [2016]

Editorial Board

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. Copyright© 2016 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

FEATURES

contents

VIEW POINT

BOOK REVIEW

PERSONALITY PROFILE

QUOTABLE QUOTES

Editorial

It has been an unforgettable period for Singapore in the last 3 months – we celebrated SAF Day on 1st July 2016 and rejoiced at our nation's 51st birthday on 9th August 2016, in a new National Stadium, no less! We also warmly cheered Joseph Schooling's historic win of Singapore's first ever Olympic Gold medal and for establishing the first Olympic Record by a Singaporean. Sadly, we also mourn the demise of our much loved President, Mr S. R. Nathan who passed away peacefully on 22nd August 2016. As Mr Peter Ong, Head of Civil Service commented, "As we mourn the loss of Mr Nathan, let us reflect on his contributions to Singapore and his unwavering dedication and tenacity in serving our country. We too can learn from him, to serve with compassion and from our heart, and always do our best to ensure Singapore's future success."[1]

In the current complex, challenging security environment, Pointer is featuring several essays which discuss how the Singapore Armed Forces (SAF) can better deal with changes and challenges in the security environment ahead. However, we should remember that we need to support the SAF in its mission to defend our home and country. Dr Ng Eng Hen, Minister for Defence said in his SAF Day Message, "But, a strong SAF is not built on hopes and aspirations alone… I ask all Singaporeans to support the SAF, with their hearts, encouragement and solidarity. What we inherited from our founding generation – our home, our Singapore – is precious and our way of life worth defending together."[2] In this issue, we present 2 essays on information warfare and one essay each on maritime security and the utility of air power for small states, respectively. We also include an essay on full spectrum operations and an analysis of the future of the SAF, in the midst of the transforming strategic, geopolitical and domestic environment.

The essay, 'To What Extent can Singapore's Maritime Security Outlook be considered as Exceptional within Southeast Asia?' is written by LTC Daniel Koh Zhi Guo. In the first part of his essay, LTC Koh discusses why Singapore's Maritime Security (MARSEC) is exceptional in the Southeast Asian region. He defines and explains what MARSEC is exactly and how it has conceptually 'widened' and 'deepened' alongside developments in Strategic Studies. He then tabulates the key MARSEC agencies of all eleven Southeast Asian states in a 'MARSEC Agencies Matrix', and examines countries that have established MARSEC institutions or agencies for the express purpose of collectively and comprehensively conducting MARSEC operations. Finally, he examines Singapore's development of the Maritime Security Task Force (MSTF), National Maritime Security System (NMSS) and Information Fusion Centre (IFC) and juxtaposes Singapore's MARSEC outlook with the fore-mentioned countries examined.

In the essay, 'Is Full Spectrum Operations a Viable Strategic Posture for the SAF?' MAJ Lee Hsiang Wei affirms that the ability to carry out full spectrum operations means that the SAF has to remain well trained in conventional war fighting, coalition operations as well as Operations Other Than War (OOTW). He points out that Singapore's diplomatic relations with other countries will be very significant for her defence. He highlights how being full spectrum capable would deter opposing forces from attacking Singapore. His essay takes into account the mission statement of the Ministry of Defence (MINDEF) and the SAF, "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." MAJ Lee concludes that for MINDEF and the SAF to achieve its mission, it is necessary for the SAF to maintain the strategic posture of full spectrum operations. However, he is aware that the ability for the SAF to maintain full spectrum operations in the future will depend on the resources available to MINDEF. In the near future, the budget allocated to MINDEF will inevitably face increasing pressures from social development sectors. In the long run, MINDEF and the SAF will need to continue to build on public trust and to be prudent in the spending of the tax dollar.

The essay, 'Cyber Attacks and the Roles the Military Can play to Support the National Cyber Security Efforts' by ME5 Alan Ho Wei Seng discusses the impact of cyber warfare to a country. He highlights that while the advent of low cost computing devices and fast access to the Internet has brought forth great convenience to everyday life, there are also many cyber threats lurking in cyberspace, waiting to exploit system or network vulnerabilities so as to compromise their integrity, availability and confidentiality. ME5 Ho stresses that on a national level, cyber attacks can exploit the vulnerabilities of critical infrastructures such as the energy, transportation and communication sectors and seriously undermine military mission success, since the infrastructures are critical in supporting the conduct of military operations. He therefore feels that there is vested interest for the military to partner with other defence agencies, private sectors and possibly international players to enable a 'whole-of-nation' effort to develop comprehensive cyber security measures in order to mitigate the impact of cyber attacks. In his opinion, this is essential as cyberspace may eventually be commonly accepted as a military domain of conflict.

The essay, 'The Future of the Singapore Armed Forces Amidst the Transforming, Strategic, Geopolitical and Domestic Environment' is written by ME5 Gabriel Lim Guang Nian. According to ME5 Lim, the strategic and political environment has transformed since the start of this century. The attacks on the United States on 9/11 have led to prolonged 'war against terror' campaigns in Afghanistan and Iraq that had international repercussions. Within the Asia-Pacific region, heightening geopolitical rivalries between great and emerging powers have resulted in regional tensions. The role of the military in non-traditional security issues such as peacekeeping, pandemics and natural disasters has become a significant area of interest for international organisations such as the United Nations (UN), states and militaries. Domestically, there have been greater diversity and expression of opinions on security, as well as the means to achieve it. The developments over the past 15 years have provided a glimpse into the challenges the SAF can face in the future. In this essay, ME5 Lim seeks to identify the future challenges facing the SAF and the means by which they may be addressed.

CPT Jeffrey Ng Zhaohong's essay, 'Information Warfare – The Challenges and Opportunities for Militaries in the Information Age' argues that owing to the globalisation of information technology, conflicts today will not only see an increase in the use of information in warfare as an operational and strategic imperative, but also in the use of information as warfare to provide non-kinetic capabilities for achieving strategic outcomes. CPT Ng then briefly examines the implications for modern militaries and concludes that the information domain will bring game-changing strategic value to militaries that can master both information in warfare and information as warfare.

Our View Point essay entitled, 'Espousing the Utility of Contemporary Air Power in the Strategic Domain for Small States' is written by LTC Victor Chen Kanghao. In this essay, LTC Chen explores how air power, defined as the ability to project military power or influence through the medium of the air to achieve strategic, operational or tactical objectives, may be utilised by the armed forces of small states like Singapore in the modern context. Firstly, using the example of Israel, he challenges critics of the early proponents of strategic bombing such as Douhet, arguing that traditional bombardment still has a decisive effect on the outcome of war, if used effectively and with precision. He then examines other strategic applications of air power for small states, namely in intelligence-gathering, psychological operations and logistics. Lastly, apart from displaying 'hard power', he contends that a strong air force may help small states accumulate 'soft power' through developing close relationships with other armed forces and engaging the international community through Humanitarian Assistance and Disaster Relief (HADR) operations.

POINTER would like to bid farewell to four key members of the POINTER Editorial Board. We wish to thank COL Lim Siong Tiong, ME7 Shue Pei Soon, LTC Huang Miaw Yee and CWO Tang Peck Hoon for their full support. POINTER has benefitted from their insightful observations on a wide variety of military subjects. POINTER would also like to extend its warmest welcome to COL Victor Huang, SLTC Goh Tiong Cheng and CWO Ng Siak Ping as they join the POINTER Editorial Board.

The POINTER Editorial Team

ENDNOTES

1. http:intranet.defence.gov.sg/miapps/AnnouncementMgr/printArticle.jsp?aid=0A63176
2. http:intranet.defence.gov.sg/miapps/AnnouncementMgr/printArticle.jsp?aid=0A62555

To What Extent can Singapore's Maritime Security Outlook be considered as Exceptional within Southeast Asia?

by LTC Daniel Kho Zhi Guo

Abstract:

The author has divided his essay into three parts where he discusses why Singapore's Maritime Security (MARSEC) is exceptional in the Southeast Asian region. Firstly, he starts by defining and explaining what MARSEC is exactly. The author then compares the outlook of MARSEC in various countries in the Southeast Asian region, namely Brunei, Indonesia, Malaysia and Thailand. Finally, the author ends with Singapore's MARSEC outlook which consists of several groups, like the National Maritime Crisis Centre, and how they are important for the defence of Singapore.

Keywords: Maritime Security; Widening; Deepening; Illegal; Co-operation

> *"Everything can be found at sea, according to the spirit of your quest."*
>
> *- Joseph Conrad*[1]

INTRODUCTION

The essay is divided into three parts. In this first part, the essay begins by examining what Maritime Security (MARSEC) is—and how it has conceptually 'widened' and 'deepened' alongside developments in Strategic Studies. I will then scope MARSEC by examining what constitutes maritime threats in praxis. I will suggest how a country's MARSEC outlook can be discerned through the extent in which it is able to comprehensively conduct MARSEC operations.

In the second part, I will then tabulate the key MARSEC agencies of all eleven Southeast Asian states in a 'MARSEC Agencies Matrix', and examine countries that have established MARSEC institutions or agencies for the express purpose of collectively and comprehensively conducting MARSEC operations.

The final part of the essay then examples Singapore's development of the Maritime Security Task Force (MSTF), National Maritime Security System (NMSS) and Information Fusion Centre (IFC) and juxtaposes Singapore's MARSEC outlook with the fore-mentioned countries examined. I will then demonstrate how Singapore's MRRSEC outlook is exceptional in Southeast Asia.

PART I: CONCEPTUALISING MARSEC

The 'Widening' And 'Deepening' Of MARSEC

The term MARSEC gained prominence in security vernacular after the catastrophic events of 11th September, 2001. The fear of terrorists crashing aircrafts into population centres and key installations was transposed onto the maritime domain, and expedited the ubiquity of the term 'MARSEC' in maritime nations all over. I will posit that the term MARSEC has evolved alongside the 'widening' and 'deepening' of thought in Security Studies.[2]

The end of the Cold War precipitated the re-theorisation of the concept of security. Accelerated by the influence of globalisation and the advent of new communications and transportation technology, contemporary conceptualisations of security have 'widened' and 'deepened'. The concept of security has been 'widened' to include threats or concerns beyond its previous narrow military domain to include the political, economic, ecological and societal.[3] In the 'deepening' of security beyond the state as its main or only referent, it has extended 'upwards' to the biosphere of supranational bodies, and 'downwards' to groups and individuals.[4]

MARSEC, I would suggest, has 'widened' in terms of navies having to contend with issues beyond war-fighting to include matters relating to customs, fishery, piracy, etc. Naval Principal Warfare Officers (PWO) honed to fight conventionally with guns, torpedoes and missiles have had to re-orientate themselves to a familiar yet operationally different environment. Navies have had to jointly enforce the law, collect evidence, learn about fishery protection and even restrain themselves from shooting at nebulous adversaries.

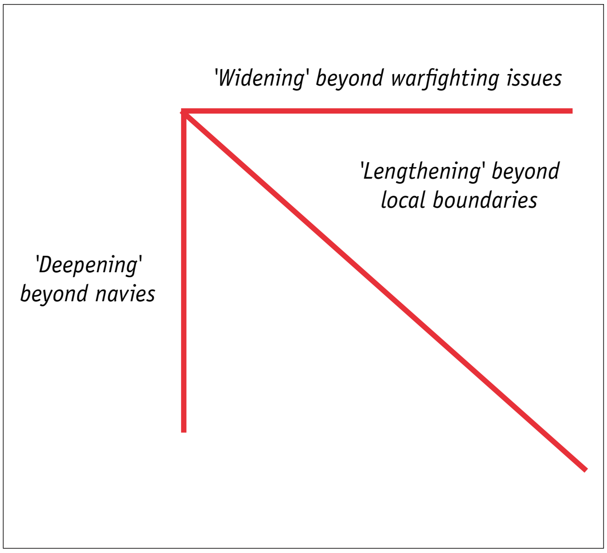

'Widening' beyond warfighting issues
'Lengthening' beyond local boundaries
'Deepening' beyond navies

Diagram 1: A Comprehensive Approach to MARSEC

MARSEC has also 'deepened' in terms of navies as its sole referent, to now include other MARSEC stakeholders as key players or partners in collaborative efforts with the navy. Vessels and personnel from the Coast Guards, Police, Customs and Fishery departments now operate, and inter-operate with their naval counterparts further and prominently from their shores. Interestingly, the traditional referent for military operations at sea reflects the change beyond semantics, from the previous Mahanian notion of 'Navy'-only operations at sea to the Corbettian concept of joint 'maritime' operations.

I suggest that MARSEC is 'post-Joint' (beyond armed services operating jointly together) and 'post-Combined' (beyond armed services from other countries operating together). MARSEC entails militaries collaborating beyond one's own shores with military and non-military enforcement agencies. MARSEC has thus conceptually 'lengthened' from the local, to the regional and the global arenas. Taking the forementioned three dimensions together, MARSEC in its praxis has 'widened', 'deepened' and 'lengthened' so that a multi-agential, trans-national or comprehensive approach is required for effective MARSEC operations. (See *Diagram 1*).

Delimiting the Boundaries of MARSEC

> *Security is "inherently a matter of dispute because no neutral definition is possible."*
>
> *– W. B. Gallie*[5]

It is germane at this juncture to scope the 'boundaries' of MARSEC before determining a country's MARSEC outlook. Admiral Robert F. Willard in his then capacity as Commander, United States Pacific Fleet (COMPACFLT), once described maritime security as an obligation that maritime stakeholders need to bear to protect the sea lanes from 'nefarious purposes'.[6]

Given the lack of a commonly used or legal definition of MARSEC, I will scope the boundaries of what MARSEC encompasses by examining what navies and other maritime security practitioners deem as 'nefarious' or 'threats' *in praxis*. I will thus attempt to harmonise what two actively engaged MARSEC agencies – Australia's Border Protection Command (BPC) and Singapore's IFC, deem as 'maritime threats'.[7] *Annex A* juxtaposes the IFC and BPC's eight stated 'maritime threats' / 'maritime concerns'. While threats may be the 'same', 'similar' or 'specific' between the two agencies, it should be noted that both the BPC and IFC exclude 'maritime boundaries' or sovereignty-related issues outside the scope of MARSEC.

MARSEC operations are therefore actions undertaken by militaries and other stakeholders nationally and beyond, to counter maritime threats prejudicial to the safe use and utilisation of the sea and its resources for national and transnational maritime interests.

Boundary-related disputes can greatly influence national, regional and even global politics.[8] The recent violent protests in Vietnam and the PLA's Lieutenant General Wang Guanzhong's response to Japanese Prime Minister Shinzo Abe and United States (US) Secretary of Defence Hagel's comments during the 2014 Shangri La Dialogue clearly attest to that.[9] I argue, however, that sovereignty-related issues are not MARSEC 'threats' per se. They can however become serious impediments to MARSEC co-operation. A case in point, is the stymied willingness to co-operate in MARSEC between Peru and Chile against drug-smuggling—a common evil along the western coast of South America.[10]

MARSEC operations are therefore actions undertaken by militaries and other stakeholders nationally and beyond, to counter maritime threats prejudicial to the safe use and utilisation of the sea and its resources for national and trans-national maritime interests.[11]

A country's MARSEC outlook, I would suggest, is the extent in which a country can comprehensively conduct effective MARSEC operations i.e. the extent in which MARSEC operations have 'widened', 'deepened' and 'lengthened'.

PART II: THE MARSEC OUTLOOK OF COUNTRIES IN SOUTHEAST ASIA

Having scoped MARSEC operations and what constitutes a country's MARSEC outlook, I will now proceed to examine the MARSEC outlook of Southeast Asian countries. Determining a country's MARSEC outlook would necessitate examining its MARSEC stakeholders and the extent they have 'widened', 'deepened' and 'lengthened' in praxis i.e. become more comprehensive in conducting MARSEC operations; For example, the extension of their navy's role to encompass traditional 'Coast Guard' duties; Marine Police and Customs being at the forefront of piracy; greater regional co-operation by MARSEC agencies with their regional counterparts, etc. (In so doing, I will focus on the operational level of MARSEC praxis, and to some extent, a country's grand strategy of apportioning scarce resources in MARSEC.)

The 'MARSEC Agencies Matrix' in *Annex B* tabulates the key MARSEC agencies, such as the Navy, Coast Guard, Marine Police, Customs and Fisheries, of all 11 Southeast Asian states. Given the scope of this essay, I will not be able to examine the respective agencies of each country in detail, but will instead examine in greater detail, countries that have established MARSEC institutions or agencies for the express purpose of collectively and comprehensively conducting MARSEC operations. (These existing

National or Regional MARSEC agencies are stated under the first two columns in the Matrix.) The countries to be examined are: Brunei, Indonesia, Malaysia, Thailand and Singapore.

The MARSEC Outlook in Brunei Darussalam

Brunei Darussalam has over 200 offshore oil and gas platforms within its Economic Exclusive Zone (EEZ). The need to continuously monitor and protect these key installations from maritime terrorism or acts of sabotage has posed a great challenge for its security and enforcement agencies. Brunei's other main maritime threats include: man-made disasters, e.g. collisions that result in massive oil spills and transnational crime 'smuggling and Illegal, Unregulated and Unreported (IUU) Fishing'.[12]

Wikipedia

KDB Darulaman at the Royal Australian Navy International Fleet Review 2013.

The Royal Brunei Navy's (RBN) small but relatively new fleet continues to grow in its conventional capacities. Its Offshore Patrol Vessels (OPV) are participating for the first time in the 24th US Pacific Fleet-hosted Rim of the Pacific (RIMPAC) exercise around the Hawaiian Islands.[13] The RBN's roles have 'widened' in the protection of offshore resources, but remain focused on developing its conventional warfighting capabilities, in which it has made some strides from its participation of its OPVs in RIMPAC.

Brunei established a National Maritime Co-ordination Centre (NMCC) in February 2010. Reporting directly to its Prime Minister Office, it seeks to create Maritime Domain Awareness and enable effective co-ordination for inter-agencies to respond to maritime threats.[14] The NMCC remains nascent however. Still in the works, is the establishment of a National Coastal Surveillance System (NCSS) for pervasive surveillance through the use of radars and remotely controlled cameras.[15] Information-sharing is conducted mainly with Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) and the IFC, and while Brunei espouses the need for a 'whole of government approach', little inter-agency coordination has been observed. In terms of 'deepening' maritime operations, the RBN remains the main and in most arenas, the sole player. Brunei's maritime institutions remain independent agencies in praxis. Regional co-operation is also limited largely to participation in the Association of Southeast Asian Nations (ASEAN)-based forums such as the ASEAN Regional Forum but is expected to 'lengthen' at least at the navy-level given its growing confidence and competency in operating technologically sophisticated fleet.

The MARSEC Outlook in Indonesia

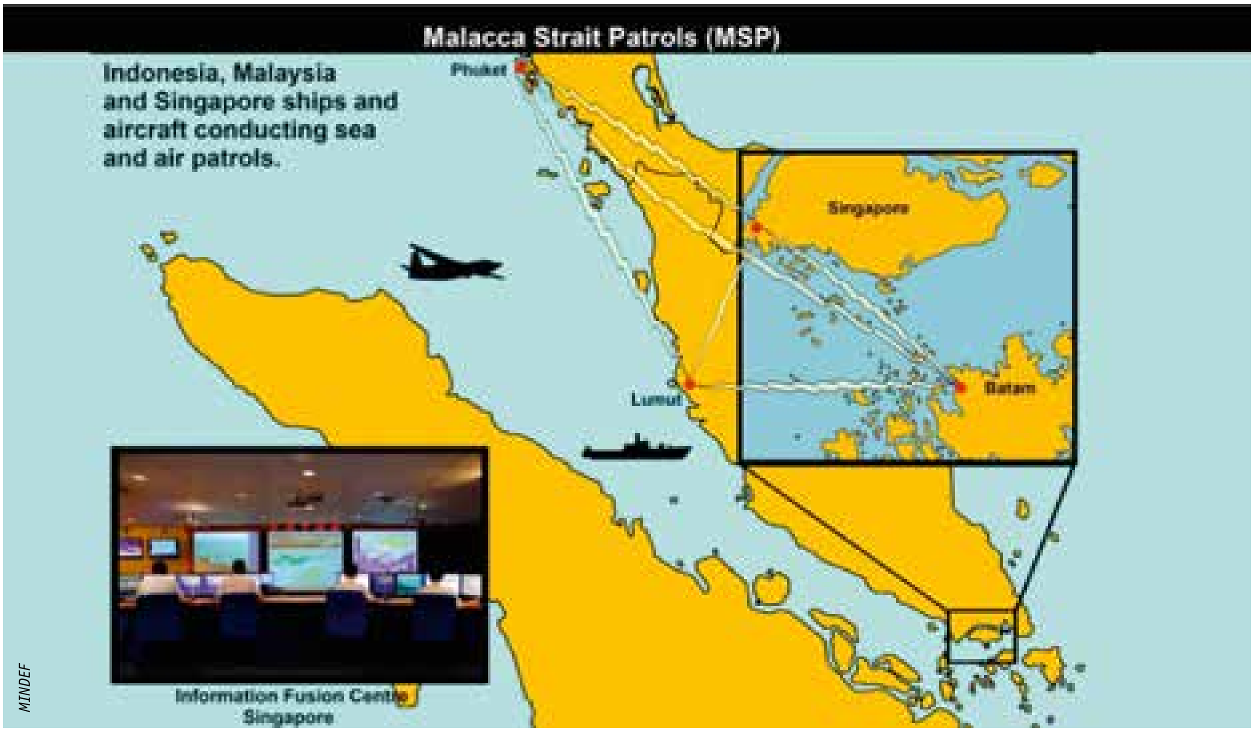
Indonesia faces significant challenges in strengthening its MARSEC given its geographical expanse of 17,500 islands and about 5.8 million square km of territorial waters.[16] Indonesia had, until recently, high rates of piracy in its waters, and together with IUU Fishing, Smuggling and Maritime Terrorism, are key Indonesian concerns in MARSEC.[17] Efforts to improve MARSEC in Indonesia through external intervention are often avoided in the fear that they may undermine Indonesia's territorial and political integrity.[18] Indonesia suffers also from the lack of a unified approach with 13 separate agencies claiming jurisdiction over the sea, including the navy and the marine police. To complicate matters further, local authorities also have MARSEC responsibilities with provinces exercising jurisdiction up to 12 nautical miles (nm) and regencies up to 3 nm.[19]

Indonesia's BAKORKAMLA was institutionalised in 2005 to establish a combined maritime agency for co-ordinating operations among stakeholders and agencies in maritime security, safety and maritime law enforcement operations in Indonesian waters.[20] The BAKORKAMLA is the pre-cursor to the establishment of an independent Coast Guard, which will be formed for the express purpose of allowing its navy, the Indonesian Navy (TNI-AL) to focus on 'defence activities' and 'not to catch fishermen'.[21] It can be argued that Indonesia is pursuing a different trajectory in MARSEC, with the TNI-AL not 'widening' its operations, but 'narrowing' instead, the spectrum of operations that the TNI-AL currently undertakes. The future Coast Guard will come to the fore and thus 'deepen' MARSEC in Indonesia as an independent service, not unlike the United States Coast Guard, capable of conducting and leading MARSEC operations with other MARSEC stakeholders.[22]

In terms of 'lengthening' MARSEC operations, regional co-operation is often hampered by sovereignty-related concerns. Indonesia for instance declined to join the US-led Proliferation Security Initiative (PSI) as it might potentially involve the interdiction by foreign navies of vessels passing through Indonesian Territorial Waters.[23] Indonesia has however pragmatically accepted help from external powers, i.e. US and Japan, in maritime capacity with the proviso that the Indonesia's sovereignty is respected.[24]

The MARSEC Outlook in Malaysia

East and West Malaysia are geographically separated by the South China Sea by a distance of about 600km at its closest point. A maritime state, Malaysia has over 4,600 km of coastline.[25] Malaysia's MARSEC landscape is further complicated by piracy in the Strait of Malacca, boundary disputes and illegal migrants with Indonesia and the Philippines. Terrorist-related activity in the form of kidnappings, such as the recent three kidnappings in three months since


Malacca Strait Patrols (MSP)
Indonesia, Malaysia and Singapore ships and aircraft conducting sea and air patrols.
Phuket
Singapore
Lumut
Batam
Information Fusion Centre Singapore

MINDEF

Infographic on the Malacca Strait Patrols.

April 2014 in Sabah, has also emphasised the need for better MARSEC to the Malaysian government.[26]

The Malaysian Maritime Enforcement Agency (MMEA) was established in 2006 by amalgamating five existing agencies into one. A sizeable fleet of patrol vessels was formed with the Royal Malaysian Navy contributing patrol crafts to form its fleet.[27] The MMEA was formed after a study in April 1999 by the Malaysian government showed that maritime related enforcement was inefficient due to the involvement of multiple agencies. The MMEA has 11 key functions, including the enforcement of law and order in 'Malaysia Maritime Zone' and the suppression of piracy, the illicit traffic of narcotic drugs and the controlling and prevention of pollution.[28]

Malaysia is similar to Indonesia in its policy of retaining its navy for defence purposes, and there is little 'widening' in the operational scope of the Royal Malaysian Navy. In the formation of a Coast Guard, the MMEA is substantively ahead and short of a name-change, is in praxis the Malaysia's functioning Coast Guard. This is very impressive given its inauguration a mere eight years ago. The MMEA is at the forefront of MARSEC operations—a clear 'deepening' in the MARSEC landscape as a strong 'parallel' maritime agency vis-à-vis its navy. The MMEA has also 'deepened' collaboration with its Marine Police.[29] Regionally, the MMEA has 'lengthened' co-operative mechanisms, including a forum for stakeholders of the Malacca Strait (including states, shipping industries, and other users) to collectively protect the maritime environment and promote the safety of navigation.

The MARSEC Outlook in Thailand

Bordering Thailand is the Andaman Sea to the west, and the Gulf of Thailand to the east. Thailand is also surrounded by the waters of several neighbouring countries, such as Vietnam, the Philippines and Malaysia. Thailand's economy is highly dependent on natural resources from the sea such as petroleum, minerals and marine living resources. The Gulf of Thailand abounds with fishing and more than 200 platforms for natural gas and crude petroleum exploitation.[30] The Andaman Sea and the Gulf of Thailand are also important Sea Lines Of Communications (SLOCs) for commerce, with up to 90% of all import and export activities conducted via the sea.[31] Maritime threats under Thailand's maritime jurisdiction include inter alia, IUU Fishing (including those undertaken by neighbouring countries); Drug Smuggling, trafficked via the Andaman Sea from its source in Myanmar; and Maritime Terrorism where terror groups in the south of Thailand have been known to (albeit rarely) attack maritime targets.[32]

Thailand's Maritime Enforcement Coordination Centre (THAI-MECC) was established in 1997 to serve as the national focal point to co-ordinate efforts among relevant Thai agencies in protecting Thailand's national interests and conducting operations in Thailand's maritime waters. The THAI-MECC reports directly to the National Security Council. The Royal Thai Navy (RTN) as the focal authority co-ordinates the operations of the four other main agencies, namely, the Marine Police, the Marine Department, the Customs Department and the Fisheries Department.[33]

The RTN has a dual role in defence and in the protection of Thailand's national maritime interests. With regards to the latter, the RTN has clearly 'widened' its scope, and is expected to perform duties such as law enforcement at sea, protection of maritime resources, hydrographic surveying, search and rescue etc.[34] In terms of 'deepening', the other four agencies co-ordinating under the ambit of the

THAI-MECC have certainly come to the fore. While they contribute their respective domain expertise in 'widening' the RTN's plethora of MARSEC operations, they are seemingly subordinate to the RTN and are not overt in undertaking MARSEC operations at sea. Their roles and responsibilities also need to be better delineated for more efficient and effective collaboration between the various agencies engaged in MARSEC.[35] Thailand has clearly 'lengthened' co-operation bilaterally, regionally and beyond. Thailand currently conducts co-ordinated patrols bilaterally with Malaysia and Vietnam along their maritime boundaries, both in the Gulf of Thailand and the Andaman Sea. The joint patrol operations are aimed, inter alia, at controlling fishery activities, protecting natural resources from violation by 'third countries', in accordance with internationally accepted principles of the law of the sea.[36] Regionally, Thailand became the fourth country to join the Malacca Strait Patrols (MSP) in September 2008, together with Indonesia, Malaysia and Singapore to enhance MARSEC in the Strait of Malacca and Singapore.[37] Beyond the region, Thailand has worked with the US in the Personal Identification Secure Comparison and Evaluation System (PISCES) and participates in the Container Security Initiative (CSI).[38]

PART III: THE MARSEC OUTLOOK IN SINGAPORE

Singapore occupies a key strategic location at the southern entrance of the Malacca Strait. One of the world's busiest ports, approximately 1,000 vessels anchor or transit in its port waters at any one time, and hundreds more ply the busy and narrow Singapore Strait. The port of Singapore is the third busiest petrochemical refinery in the world and a major container transhipment hub, in the intricate just-in-time global manufacturing system upon which global commerce depends.[39] A maritime terrorist strike on its port facilities would have severe regional and global repercussions, and seriously affect Singapore given its dependence on external trade. In addition to its vulnerabilities, Singapore is also a prime target for radical Islamist terrorists on account of serving host to thousands of Western multinational companies, and its close security links to the US and Israel. Islamist terror groups, such as the Jemaah Islamiyah (JI) planned to attack US military personnel and naval vessels in Singapore as part of its bomb plots in Singapore post-9/11 in 2001.[40] Maritime threats for Singapore are narrow, and principally centre on Maritime Terrorism and SLOC security.

> *The port of Singapore is the third busiest petrochemical refinery in the world and a major container transhipment hub, in the intricate just-in-time global manufacturing system upon which global commerce depends. A maritime terrorist strike on its port facilities would have severe regional and global repercussions, and seriously affect Singapore, given its dependence on external trade.*

The Maritime Security Task Force: 'Widening' Singapore's MARSEC

The MSTF was established in 2009 as part of Singapore's 'Whole-of-Government' (WOG) approach to MARSEC. It was formed in recognition that would-be perpetrators may exploit inter-agency gaps in the independent silos that maritime agencies often operate in. Formed with ships and personnel from the Republic of Singapore Navy's (RSN) Coastal Command (COSCOM), the MSTF is a standing Singapore Armed Forces (SAF)-level that is able to marshal forces from the SAF to form an integrated task force to execute security operations, in co-ordination with other national maritime agencies. The MSTF is also responsible for developing and maintaining maritime domain awareness and collaborating with other national maritime agencies.[41]

The RSN has clearly 'widened' its reach with the formation of the MSTF and MARSEC Command.[42] Singapore's waters are monitored 24/7 with integrated RSN, Maritime and Port Authority of Singapore (MPA) and Police Coast Guard (PCG) radars and cameras that are assessed via C4I systems with powerful algorithms that flag up anomalies. Ships are threat-evaluated with pre-arrival information from the MPA before they enter Singapore's port waters. RSN Patrol Vessels, PCG boats and Accompanying Sea Security Team (ASSeT) (comprising mixed teams of RSN and PCG boarding personnel) are then accordingly cued to deter and prevent potential belligerents.

It is necessary for Singapore and the rest of Southeast Asia to rise above historical interstate rivalries and mutual suspicions that have hitherto limited a cohesive regional response to regional security challenges.

Quite evidently, the MARSEC has also 'deepened' with MARSEC stakeholders collaborating with the RSN. MARSEC-stakeholders, such as the MPA and the Immigration and Checkpoint Authority (ICA) have also implemented a range of regulatory measures, including the re-routing of shipping routes and the use of the Harbour Craft Transponder System (HARTS). The key players in MARSEC are clearly not just from Singapore's Navy.

The National Maritime Security System: 'Deepening' Singapore's MARSEC

The establishment of the National Maritime Security System (NMSS) was the next concrete step in forging a WOG approach and in demonstrating the extent in which MARSEC has 'deepened' in Singapore. The NMSS consists of two entities or 'groups', the National Maritime Sense-making Group (NMSG) and the National Maritime Operations Group (NMOG) operating in tandem at the National Maritime Co-ordination Centre (NMCC), which is co-located with MSTF HQ and the Port Operations Control Centre (POCC) at the Changi Command and Control Centre.

The NMSG and NMOG comprise personnel seconded from Singapore's key maritime stakeholder agencies, namely, the RSN, Singapore Police Force (SPF), the ICA, and Singapore Customs (SC). On a daily basis, the NMSG collates information from the respective agencies' and 'open' sources, 'sense-makes' the disparate information through their professional expertise, and in 'joining the dots', generate actionable information to cue the NMOG and their various parent agencies. In a similar fashion, NMOG members collaboratively generate operation plans based on the information cues provided by NMOG as well as in anticipation of upcoming events that may require the co-ordination of enhanced maritime security operations. Both the NMSG and the NMOG serve also to build capacity in terms of developing sense-making, and Command and Control (C2) communication systems. In a maritime crisis, NMSG and NMOG serve to support the nationally designated Incident Managers in co-ordinating a collective response to the exigencies at sea.

The Information Fusion Centre: 'Lengthening' Singapore's MARSEC

The IFC was inaugurated in 2009 to foster MARSEC co-operation in the region and beyond, and manifestly

Details of the MH370 Search and Locate operation being shared among various International Liaison Officers at the Information Fusion Centre.

sets Singapore apart in how it has 'lengthened' operationally. Comprising RSN and International Liaison Officers (ILOs) across the globe from different parent agencies like Customs, Immigration, Defence, etc., the ILOs serve as conduits between the IFC and their respective nation-parent agencies.[43] The IFC operates as a maritime information hub with extensive links to 64 agencies in 34 countries.[44] It has a common maritime picture collated from various information sources, both through its partners as well as through new technologies such as the satellite-based Automatic Information System (AIS) and Long Range Identification Tracking System (LRIT). Information sharing portals, such as the Regional Maritime Information Exchange (ReMix) and the Malacca Straits Patrol Information System (MSP IS) can be tailored to allow relevant information in the form of a common maritime picture, reports and pictures to be exchanged and enable real-time collaboration through 'chat'. The IFC also organises MARSEC workshops and hosts the Shared Awareness Meeting, where members of the shipping community gather and share MARSEC-related concerns. The IFC also organises information-sharing exercises, such as the bi-annual Maritime Information Sharing Exercise (MARISX). A total of 72 International Liaison Offices and 38 Operation Centres from 30 countries participated in in the scenario-driven shore-based MARISX 2013.[45]

CONCLUSION

I have posited that a country's MARSEC outlook is the extent in which a country can comprehensively conduct effective MARSEC operations. One can argue that Singapore's MARSEC outlook is exceptional in Southeast Asia, by the extent in which it has 'widened', 'deepened' and 'lengthened' its ability to conduct MARSEC operations.

In 'widening' the RSN, Singapore has capitalised on its navy through the MSTF, in a region that is unlikely to see conventional conflict. This is due in no small part to the RSN's ability to achieve and maintain competency in conventional, three-dimensional and joint warfare competencies. While Brunei's navy will foreseeably join the ranks of its neighbours with a strong and competent navy, Brunei can be expected in the meantime, to prioritise its scarce human resources into strengthening the RBN, and apportion less time and energy to the development of its NMCC.

In 'deepening' Singapore's MARSEC, the island-city state has bridged its silos by bringing together stakeholders in the maritime domain. In so doing, Singapore has effectively fostered a truly WOG approach to MARSEC through the MSTF and the NMSS with its crew of seconded personnel from key MARSEC stakeholders. While Indonesia and Malaysia's formation of the BAKORKAMLA and MMEA respectively, have and will, continue to improve operational co-ordination, it is a Coast Guard that they eventually will establish. Depending on whether BARKORKAMLA will continue to co-ordinate operations among MARSEC stakeholders, there is foreseeably a need for both countries to create a separate body to bring together their respective navies and MARSEC stakeholders, including non-military/enforcement type agencies. While the Thai-MECC has been established for 17 years, the rest of the other MARSEC-related agencies need to step up to plate, and clarify their roles and responsibilities to enhance collaboration between the various agencies engaged in MARSEC.

In terms of 'lengthening' MARSEC, Singapore's IFC remains the only information-sharing agency of its type with ILOs from the region operating together as a maritime information-sharing hub with extensive linkages all over the world. Noteworthy as well, are the IFC's numerous engagements with the shipping industry. Singapore is also relatively unencumbered by issues of sovereignty unlike Indonesia and Malaysia. Not unlike Thailand, it is a strong supporter of extra-regional initiatives in enhancing MARSEC, especially US-led initiatives like the Container Security Initiative to screen containers and cargo bound for US ports, and the US Coast Guard-led IPSP, under which the USCG can inspect Singapore's port facilities and verify its implementation of the ISPS Code.[46]

Singapore, in its quest to survive its vulnerabilities and remain strategically relevant as a maritime nation, has effectively and efficiently planned and calibrated its resources, technology and infrastructure to comprehensively conduct MARSEC operations. While Singapore may be exceptional thus far, its fate does not remain wholly in its hands, and just as maritime threats are trans-agency, they are trans-boundary. It is necessary for Singapore and the rest of Southeast Asia to rise above historical interstate rivalries and mutual suspicions that have hitherto limited a cohesive regional response to regional security challenges.[47]

ANNEX A : COMPARISON OF MARITIME THREATS BETWEEN THE IFC AND BPC

Threat Category (T)	INFORMATION FUSION CENTRE[48]	BORDER PROTECTION COMMAND[49]
1	Smuggling/ Trafficking/ Contraband	Prohibited Imports / Exports
2	Irregular Human Migration	Irregular Maritime Arrivals
3	Illegal Fishing	Illegal Exploitation of Natural Resources
4	Maritime Incidents[50]	Marine Pollution
5	Natural Events	Compromise to Bio-Security
6	Piracy/ Sea Robbery/ Sea Theft	Piracy, Robbery or Violence at Sea
7	Possession of Illegal Weapons	Illegal Activity in Protected Areas
8	Maritime Terrorism	Maritime Terrorism

Both agencies have Threats that are clearly the 'same', such as Smuggling (T1), Piracy/Sea Robbery (T6) and Maritime Terrorism (T8). They have 'similar' Threats as well (T2, T3 and T4), although each agency may have a broader understanding of what that threat category encompasses. The BPC's concern for 'Illegal Exploitation of Natural Resources' (T3) for instance, extends beyond fish stocks to include oil and gas. There are also Threats that are 'specific' to each agency as well, such as the 'Possession of Illegal Weapons' (T7) for the IFC and the 'Compromise to Bio-security' for the BPC. While Threats may be the 'same', 'similar' or 'specific' (3 'S') between two or more agencies, it should be noted that both the BPC and IFC exclude 'maritime boundaries' or sovereignty-related issues outside the scope of MARSEC.

ANNEX B: MARSEC AGENCIES MATRIX (SOUTHEAST ASIA)

S/N	SEA COUNTRY	Regional MARSEC Agency	National MARSEC Agency	Navy	COAST GUARD	MARINE POLICE	CUSTOMS	FISHERIES	COASTAL RESOURCES
1	Brunei	_	National Maritime Coordination Centre (NMCC)	Royal Bruneian Navy (RBN)	_	Marine Police	Royal Customs and Excise Dept	Dept of Fisheries	_
2	Cambodia	_	_	Royal Cambodian Navy	_	_	Royal Customs and Excise Dept	Ministry of Agriculture, Forestry and Fisheries	_
3	East Timor	_	_	F-FTDL (Naval Component) / East Timor Navy	_	Marine Police (PNTL)	Dept of Customs	Ministry of Agriculture, Forestry and Fisheries	_

S/N	SEA COUNTRY	Regional MARSEC Agency	National MARSEC Agency	Navy	COAST GUARD	MARINE POLICE	CUSTOMS	FISHERIES	COASTAL RESOURCES
4	Indonesia	_	BAKORKAMLA	TNI-AL	_	POLRI	Dept of Customs	Dept of Fisheries	Dept of Energy and Mineral Resources
5	Laos	_	_	Lao People's Navy (LPN)	_	_	Dept of Customs	Dept of Livestock & Fisheries (DOLF)	Dept of Marine and Coastal Resources
6	Malaysia	_	_	Royal Malaysian Navy (RMN)	Malaysian Maritime Enforcement Agency (MMEA)	Marine Police	Royal Malaysian Customs Dept	Dept of Fisheries	_
7	Myanmar	_	_	Mynamar Navy	Coast Guard wing in Navy for Fisheries Dept	Myanmar Marine Police (MPF)	Dept of Customs	Dept of Fisheries	_
8	The Philippines	_	National Coast Watch System (Policy-level)	Philippine Navy	Philippine Coast Guard	Maritime Command (MARICOM)	Bureau of Customs	Bureau of Fisheries and Aquatic Resources	_
9	Singapore	Information Fusion Centre	National Maritime Crisis Centre (NMCC)	Republic of Singapore Navy (RSN)	_	Singapore Police Coast Guard (PCG)	Singapore Customs; Immigration & Customs	Agri-Food & Veterinary Authority (AVA) - Marine Fisheries Research Dept	_
	_	_	Maritime Security Task Force (MSTF)		Authority (ICA)	_	_	_	_
10	Thailand	Maritime Information Sharing Centre (MISC)	Thai-Maritime Enforcement Coordinating Centre	Royal Thai Navy (RTN)	_	Royal Thai Marine Police	Dept of Customs	Dept of Fisheries	Dept of Marine & Coastal Resources
11	Vietnam	_	_	Vietnamese People Navy	Vietnam Coast Guard	Vietnam Marine Police	General Dept of Vietnam Customs	Ministry of Agriculture and Rural Development (MARD); Vietnam Fisheries Resources Surveillance Dept	_

BIBLIOGRAPHY

Border Protection Command, http://www.bpc.gov.au/site/page5777.asp.

Defence Market Intelligence, 2013. http://dmilt.com/index.php?option=com_content&view=article&id=6507:brunei-mod-issues-rfi-for-coastal-surveillance-layout&catid=3:asia&Itemid=56.

CIA, *The World Fact Book*, https://www.cia.gov/library/publications/the-world-factbook/geos/id.html.

Council on Foreign Relations, 2014. http://www.cfr.org/asia-and-pacific/remarks-chinese-lieutenant-general-wang-shangri-la-dialogue/p33054.

The Jakarta Post, 2010. http://www.thejakartapost.com/news/2010/06/25/indonesia-plans-establish-independent-coast-guard-soon.html.

Joshua Ho, ed., Realising Safe and Secure Seas for All: International Maritime Security Conference 2009, (Singapore: *Select Publishing*, 2009).

Kate Hodal, "At least 21 dead in Vietnam anti-China protests over oil rig", (*The Guardian*, 2015). http://www.theguardian.com/world/2014/may/15/vietnam-anti-china-protests-oil-rig-dead-injured.

Tim Lynch, "MMEA: A Modern Coast Guard", FrontLine Security, v._ 7, n._ 1, 23-24.

MINDEF website: IFC Fact Sheet. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2014/apr/04apr14_nr/04apr14_fs.html#.U6aTu42Sx38

MINDEF website: Maritime Information-sharing Exercise Fact Sheet http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2013/may/14may13_nr/14may13_fs.html#.U6aVE42Sx38.

Captain Suriya Pornsuriya, Royal Thai Navy, "Maritime Terrorism: Thailand's Perspective" in a paper represented at the Workshop on Maritime CounterTerrorism, 29 – 30 November 2004, New Delhi, India, organized by the Observer Research Foundation. http://www.observerindia.com/cms/sites/orfonline/modules/report/ReportDetail.html?cmaid=1310&mmacmaid=1285.

Waquiddin Rajak, "Brunei Navy Ships to Join US Exercise", (*The Brunei Times*, 2014). http://www.bt.com.bn/frontpage-news-national/2014/05/13/brunei-navy-ships-join-us-exercise.

Michael Richardson, "Singapore welcomes US aircraft carrier", (*International Herald Tribune*, 2001). http://www.singapore-window.org/sw01/010322ih.htm.

Steve Smith, "The Contested Concept of Security" in *IDSS Commentaries Paper*, n._ 23, 2002.

Andrew T. H. Tan (2011) *Security Strategies in the Asia-Pacific* (New York: Palgrave, Macmillan).

Rear Admiral Tan Wee Beng, RSN, "Enhancing Maritime Security through Singapore's Maritime Security Task Force (MSTF) in Joshua Ho, ed., (2009) Realising Safe and Secure Seas for All: International Maritime Security Conference 2009 (Singapore: Select Publishing).

Till, *Seapower: A Guide for the Twenty-first Century* (New York: Routledge, 2013).

Ubadillah Masli, "To keep an eye on Brunei's waters", (*The Brunei Times*, 2011). http://www.bt.com.bn/news-national/2011/07/30/keep-eye-brunei-waters.

Wall Street Journal, "Gunmen Kidnap Fish-farm Workers in Malaysia", 2014. http://online.wsj.com/articles/gunmen-kidnap-fish-farm-workers-in-malaysia-1402903288.

Lieutenant General Wang Guanzhong, PLA-N China, "Remarks by Chinese Lieutenant General Wang at the Shangri-La Dialogue".

CDR Yodyooth Wongwanich & LCDR Ekgarat Narkmee, Royal Thai Navy, "The Enhancement of Thailand's Maritime Security Cooperation" in "The Information Fusion Centre: Challenges and Perspectives", *POINTER*, 2011.

ENDNOTES

1. Joseph Conrad, "A Personal Record", 1912.

2. Steve Smith, "The Contested Concept of Security" in *IDSS Commentaries Paper*, n._23, 2002.

3. Barry Buzan, Ibid.

4. Ibid.

5. W. B. Gallie, "Essentially Contested Concepts", *Proceedings of the Aristotelian Society*, Vol.56, (1956), p. 167–198.

6. Joshua Ho, ed., Realising Safe and Secure Seas for All: International Maritime Security Conference 2009 (Singapore: *Select Publishing*, 2009), 76.

7. The IFC is also veritably a trans-national/ regional agency, in addition to being multi-agency. The IFC will be further elaborated.

8. It is necessary in scoping "MARSEC" to briefly address the deliberate exclusion of sovereignty-related issues given their significance in Southeast Asia and the South China Sea in recent years.

9. Kate Hodal, “At least 21 dead in Vietnam anti-China protests over oil rig”, *The Guardian*, 2015, http://www.theguardian.com/world/2014/may/15/vietnam-anti-china-protests-oil-rig-dead-injured.

   Lieutenant General Wang Guanzhong, PLA-N China, “Remarks by Chinese Lieutenant General Wang at the Shangri-La Dialogue”, *Council on Foreign Relations*, 2014. http://www.cfr.org/asia-and-pacific/remarks-chinese-lieutenant-general-wang-shangri-la-dialogue/p33054.

10. Shared by the IFC’s Peruvian ILO during the Regional MARSEC Practitioner Course 2014, held in the Changi C2 Centre, Singapore from 2 to 6 June 2014.

    In contrast, Singapore and Malaysia placed aside their territorial disputes during the “SOMS Terror Alert” to deter and avert the oil tanker terror alert in March 2010.

11. I have adapted my definition of MARSEC operations from the Royal Navy. It defines it as “actions performed by military units in partnership with other government departments, agencies and international partners in the maritime environment to counter illegal activity and support freedom of the seas, in order to protect national and international interests”. *Till Seapower: A Guide for the Twenty-first Century* (*New York: Routledge*, 2013), 283.

12. Based on Director of NMCC, COL Nooradin Yaakob’s presentation during the 10th ARF ISM on Counter-terrorism and Transnational Crime in Hoi An, Vietnam, held from 16 to 17 Mar 2012.

13. Comprising fast patrol boats, the IJIHTIHAD Class Inshore Patrol vessel and the DARUSSALAM Class, Offshore Patrol Vessels (PVs).

    Waquiddin Rajak, “Brunei Navy Ships to Join US Exercise”, (The Brunei Times, 2014), http://www.bt.com.bn/frontpage-news-national/2014/05/13/brunei-navy-ships-join-us-exercise.

14. Ibid.

15. *Defence Market Intelligence*, http://dmilt.com/index.php?option=com_content&view=article&id=6507:brunei-mod-issues-rfi-for-coastal-surveillance-layout&catid=3:asia&Itemid=56.

    Ubadillah Masli, “To keep an eye on Brunei’s waters”, (*The Brunei Times*, 2011), http://www.bt.com.bn/news-national/2011/07/30/keep-eye-brunei-waters.

16. Andrew T. H. Tan *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 101; CIA, The World Fact Book, https://www.cia.gov/library/publications/the-world-factbook/geos/id.html.

17. The crisis of governance after the fall of the Suharto regime in 1998 was marked by political and social instability and a severe economic crisis. Ethnic and religious conflict broke out throughout the Indonesian archipelago (e.g Aceh, Kalimantan, West Papua, Maluku) and raised fears of the possible fragmentation of the Indonesian state. It was from within this crucible of territorial and political strife that the radical Islamist group, the Jemaah Islamiyah (JI) emerged. Andrew T. H. Tan (2011) *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 101.

18. It is important to note that Indonesia’s perspective on MARSEC is conditioned by geography and its defense doctrine of *Wawasan nusantra* i.e. to maintain its far-flung archipelago in one unitary state.

19. Andrew T. H. Tan, Security Strategies in the Asia-Pacific (New York: Palgrave, *Macmillan*, 2011), 102.

20. These 12 stakeholders include: the Ministry of Defense, Ministry of Justice and Human Rights, Heads of State Police, Heads of State Intelligence etc. MARSEC Agencies not reflected in the MARSEC Agencies Matrix in Annex A, include “Sea Transportation” and “National Education”.

21. Andrew T. H. Tan *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 102.

    The Jakarta Post, 2010. http://www.thejakartapost.com/news/2010/06/25/indonesia-plans-establish-independent-coast-guard-soon.html

22. Ibid.

23. Andrew T. H. Tan, *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 104.

24. The US has helped establish an integrated maritime surveillance system in the SOMS with 12 coastal surveillance stations equipped with radar, ship-identification systems, long-range cameras and communication systems. Japan has also provided training and equipment in the areas of immigration control, customs cooperation and measures against

terrorism financing. Andrew T. H. Tan, *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 103-104.

25. Ibid. 104-105.

26. "Gunmen Kidnap Fish-farm Workers in Malaysia", *Wall Street Journal*, 2014, http://online.wsj.com/articles/gunmen-kidnap-fish-farm-workers-in-malaysia-1402903288.

27. Andrew T. H. Tan Security Strategies in the Asia-Pacific (New York: Palgrave, *Macmillan*, 2011), 105. The Navy contributed some 70 patrol crafts, with the MMEA purchasing an additional 38 Rigid Hull Inflatable Boats (RHIBs) to augment its fleet.

28. Tim Lynch, "MMEA: A Modern Coast Guard", *FrontLine Security*, v._ 7, n._ 1, 23-24.

29. Ibid. In 2013, the Marine Police transferred 61 boats, some marine bases and personnel to the MMEA.

30. Captain Suriya Pornsuriya, Royal Thai Navy, "Maritime Terrorism: Thailand's Perspective" in a paper represented at the Workshop on Maritime CounterTerrorism, 2004, New Delhi, India, organized by the Observer Research Foundation. http://www.observerindia.com/cms/sites/orfonline/modules/report/ReportDetail.html?cmaid=1310&mmacmaid=1285.

31. CDR Yodyooth Wongwanich & LCDR Ekgarat Narkmee, Royal Thai Navy, "The Enhancement of Thailand's Maritime Security Cooperation" in "The Information Fusion Centre: Challenges and Perspectives", *POINTER*, 2011, 43.

32. Ibid.

33. Ibid.

34. Captain Suriya Pornsuriya, Royal Thai Navy, "Maritime Terrorism: Thailand's Perspective" in a paper represented at the Workshop on Maritime CounterTerrorism, 2004, New Delhi, India, organized by the Observer Research Foundation. http://www.observerindia.com/cms/sites/orfonline/modules/report/ReportDetail.html?cmaid=1310&mmacmaid=1285.

35. CDR Yodyooth Wongwanich & LCDR Ekgarat Narkmee, Royal Thai Navy, "The Enhancement of Thailand's Maritime Security Cooperation" in "The Information Fusion Centre: Challenges and Perspectives", *POINTER*, 2011, 47.

36. Captain Suriya Pornsuriya, Royal Thai Navy, "Maritime Terrorism: Thailand's Perspective" in a paper represented at the Workshop on Maritime CounterTerrorism, 2004, New Delhi, India, organized by the Observer Research Foundation.

37. The MSP comprising the Malacca Strait Sea Patrol (MSSP), the "Eyes-in-the-Sky" air patrols as well as the Intelligence Exchange Group (IEG), is a set of practical measures undertaken to ensure the security of the SOMS.

38. Captain Suriya Pornsuriya, Royal Thai Navy, "Maritime Terrorism: Thailand's Perspective" in a paper represented at the Workshop on Maritime CounterTerrorism, 2004, New Delhi, India, organized by the Observer Research Foundation.

39. Andrew T. H. Tan, *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 108.

40. The Republic of Singapore Navy's Changi Naval Base welcomed its first US aircraft carrier, USS Kitty Hawk in March 2001, and remains a key stopover for US warships and nuclear-powered air-craft carriers today. Michael Richardson, "Singapore welcomes US aircraft carrier", (*International Herald Tribune*, 2001). http://www.singapore-window.org/sw01/010322ih.htm.

41. The MSTF's concept of operations comprises three prongs: (1) To establish Comprehensive Maritime Awareness; (2) To effect Calibrated and Flexible Operations; and (3) To coordinate with other SAF units and national maritime agencies, and to collaborate with international partners and the shipping community. Rear Admiral Tan Wee Beng, RSN, "Enhancing Maritime Security through Singapore's Maritime Security Task Force (MSTF) in Joshua Ho, ed., *Realising Safe and Secure Seas for All: International Maritime Security Conference 2009* (Singapore: Select Publishing, 2009), 187-188.

42. MARSEC Command is the navy formation under which subordinate naval squadrons (e.g the Patrol Vessel Squadron) Raise, Train and Sustain (RTS) units to undertake MSTF and other naval operations. Commander MSTF is also concurrently Commander MARSEC.

43. "The Information Fusion Centre: Challenges and Perspectives", *Pointer*, 2011, 6.

44. *MINDEF* website: IFC Fact Sheet. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2014/apr/04apr14_nr/04apr14_fs.html#.U6aTu42Sx38.

45. *MINDEF* website: Maritime Information-sharing Exercise Fact Sheet. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2013/may/14may13_nr/14may13_fs.html#.U6aVE42Sx38.

46. Andrew T. H. Tan, *Security Strategies in the Asia-Pacific* (New York: Palgrave, *Macmillan*, 2011), 111.

47. Ibid, 95.

48. Ibid, 4. These IFC "key concerns" were tabulated based on presentations by Southeast Asian nations at the RSIS "Maritime Risk Conference" held in 2010. They were not explicitly categorised into the stated eight concerns, and are by no means necessarily static. Maritime boundaries are for instance, not expressed as a key concern for the Philippines when the monograph was promulgated. These eight 'key concerns' have however remained largely constant over the years and reflect the collective areas of expressed interest by the International Liaison Officers attached at the IFC. These 'maritime threat' categories scope the IFC's areas of information sharing and research. Incidents that fall under these eight categories are also reported in the IFC's Daily Ops Brief reports which are made available to their home countries and parent agencies.

49. Australian Government. Department of Immigration and Border Protection. http://www.bpc.gov.au/site/page5777.asp.

50. Usually pollution and environmental-related incidents, as well as any other incident that does not fall under any of the other seven categories (e.g. "insider" siphoning of marine fuel), or an incident still under investigation.

LTC Daniel Koh Zhi Guo graduated from the University of Birmingham with a Bachelors of Science in Political Science and Sociology with 1st Class Honours and a Masters of Science in Strategic Studies under the Continuing Education Masters Programme with the S. Rajaratnam School of International Studies (RSIS). He also graduated as the Distinguished Graduate from the 45th Command and Staff Course at the Goh Keng Swee Command and Staff College. LTC Koh is a Naval Combat Officer by vocation and served on board Landing Ship Tanks, Patrol Vessels (PV) and at the Maritime Security Task Force as a Staff Officer. He commanded a PV, RSS *Justice*, and is currently Executive Officer/Chief Instructor of Midshipman Wing, OCS. This essay won a Commendation Award in the 2014/15 Chief of Defence Force Essay Competition.

Is Full Spectrum Operations a Viable Strategic Posture for the Singapore Armed Forces?

by **MAJ Lee Hsiang Wei**

Abstract:

The author states that the ability to carry out full spectrum operations means that the Singapore Armed Forces (SAF) has to remain well trained in conventional war fighting, coalition operations as well as Operations Other Than War (OOTW). He also points out that Singapore's diplomatic relations with other countries would be very significant for her defence. He highlights how being full spectrum capable would deter opposing forces to attack Singapore. His essay takes into account the mission statement of the Ministry of Defence (MINDEF) and the SAF, "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." The author concludes that for MINDEF and the SAF to achieve its mission it is necessary for the SAF to maintain the strategic posture of full spectrum operations. However, he is aware that the ability for the SAF to maintain full spectrum operations in the future would depend on the resources available to MINDEF. In the near future, the budget allocated to MINDEF will inevitably face increasing pressures from social development sectors. In the long run, MINDEF and the SAF will need to continue to build on the public trust and to be prudent in the spending of the tax dollar.

Keywords: Deterrence; Diplomacy; Swift and Decisive Victory; Budget; Full Spectrum

INTRODUCTION

The ability to carry out full spectrum operations means that the SAF has to remain well trained in conventional war fighting, coalition operations as well as OOTW. In 2005, Mr Teo Chee Hean, then Minister for Defence, highlighted in a speech at SAFTI Military Institute that in addition to honing the conventional war fighting skill set, "3rd Generation SAF officers must be prepared for a wider spectrum of operations. They will have to operate with other national security and civil agencies, with coalition partners, with Non-Government Organisations (NGO) in the glare of the global media."[1]

The question whether full spectrum operations is a viable strategic posture for the SAF or having to choose any one of the component military operational skill sets needs to be answered at both a needs as well as a resource perspective.

This essay will take into account the mission statement of MINDEF and the SAF, "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."[2]

Let's look at the argument that maintaining full spectrum operations is a necessity rather than a question of viability. It would only be foolhardy for the SAF to choose to focus on any one of the military operational skill sets. Despite the necessity for the SAF to maintain full spectrum operations, the budget allocation for MINDEF in the future years will face pressures from other needs of the Singapore population and the SAF would need to continue to build on the public trust and find innovative and creative means to reap greater returns on each defence dollar spent. From the mission statement, it is easy to understand that the SAF seeks to ensure Singapore's peace and security via a three-pronged strategy – (1) deterrence, (2) diplomacy and (3) a swift and decisive victory as seen in *Figure 1*.

Participating in these missions is as much about showing competence of the SAF as it is about sharing skills or building patterns of operational predictability and communication.

DETRRENCE

The concept of military deterrence is the use of threats by one state to convince another to refrain from initiating a specific military action.[3] The Director of Military Sciences at the Royal United Services Institute, Michael Codner, argued that military deterrence could only be achieved when the user state has established the perception of capability to deliver a military outcome. The perception of will and reputation of the ability to implement intentions effectively are also important elements of military deterrence.[4] For the SAF to achieve deterrence over potential aggressors, there is a need to participate in coalition operations and OOTW. In these missions, these soldiers serve as ambassadors for the nation. The soldiers' vigilance, skill and adaptability in unfamiliar environments enhance the SAF's reputation as a professional outfit.[5] Through positive displays, the SAF can build a positive reputation which would act as deterrence against potential aggressors. Participating in these missions is as much about showing competence of the SAF as it is about sharing skills or building patterns of operational predictability and communication.[6]

DIPLOMACY

Defence diplomacy serves specific foreign and security policy objectives. It creates sustainable co-operative relationships, thereby building trust and facilitating conflict prevention.[7] Mr. Kwa Chong Guan, Head of External Programmes at the S. Rajaratnam School of International Studies (RSIS), described that defence diplomacy had become an important tool of a state's foreign and security policy, a result of rising

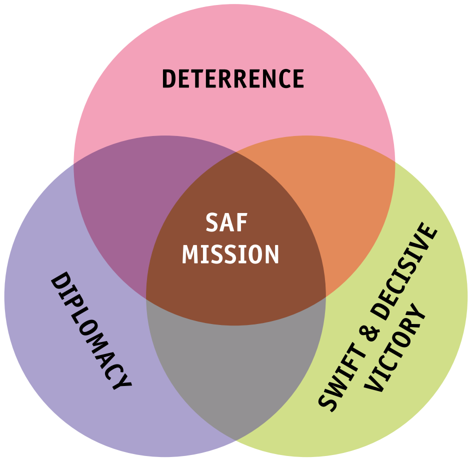


Figure 1: SAF Mission

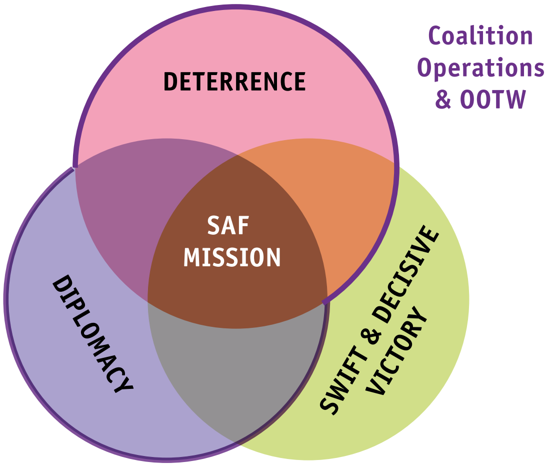


Figure 2: Coalition Operations & OOTW

reliance and appreciation among states of multilateral avenues to discuss security issues both at the regional and international levels.[8] The valuable contributions of SAF personnel in coalition operations and OOTW reflect the transnational nature of the security challenges we now face. Such operations allow the SAF to further selected international agendas that the SAF is unable to carry out alone. The Operation Blue Sapphire (OBS) missions to the Gulf of Aden to combat piracy is an example of the SAF protecting Singapore's interests as part of the larger international agenda. Lieutenant Colonel (LTC) Richard Lim, then Deputy Commander of the Combined Task Force 151 to the Gulf of Aden in 2010, aptly argued that:

Given these preconditions, the need for the SAF to be able to achieve a swift and decisive victory is one of necessity and basic survival.

> *"The deployment of a Task Group to an area 4,000 nm from home could not have more strongly underscored Singapore's oft-stated position that ensuring maritime security in the key waterways of the world cannot be the province of any State acting alone. Rather, it requires the commitment of all stakeholders including littoral states, user states, industry as well as members of the international community."*[9]

In today's interconnected world, it is expected that all countries must do their part to maintain security and stability and Singapore is a responsible member of the international community.[10] Participating in both coalition and OOTW missions allows for the SAF to not only become a respected member of the international defence community but also to punch above her weight and keep the major powers engaged in the region to promote stability.[11]

SWIFT AND DECISIVE VICTORY

The ability to ensure a victory in any conflict and to protect the country's interests is the bread and butter of any armed force.[12] Caspar Weinberger, the Secretary of Defence to President Ronald Regan, argued in a speech in 1984 that the assurance of the nation's survival and protection of its interests lies solely on its armed forces and its security policy.[13] The SAF is no different and hence the SAF needs to always be well trained in conventional war fighting. Singapore has structural vulnerabilities stemming from its small size in landmass, population and virtual lack of natural resources.[14] For the SAF to engage an aggressor in a protracted war is disadvantageous. Given these preconditions, the need for the SAF to be able to achieve a swift and decisive victory is one of necessity and basic survival.

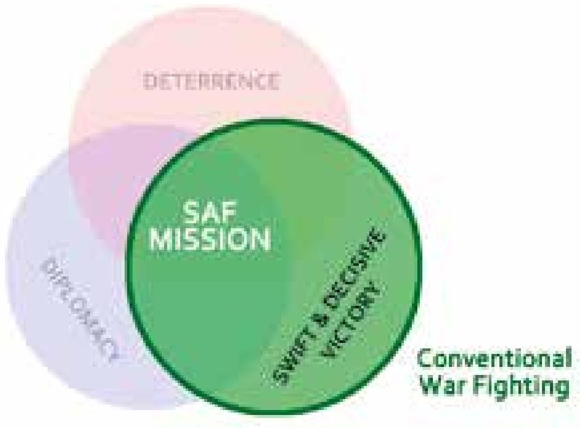


Figure 3: Conventional War Fighting

CAN SAF AFFORD TO CHOOSE JUST ONE OF THE MILITARY OPERATIONAL SKILL SETS?

From the use of the term "should these fail" in SAF's mission statement, one can infer that the "swift and decisive victory" is viewed a last resort. Some may argue that the SAF can just rely on this 'last resort' and focus wholly on the conventional war fighting skill set. This strategic posture is not viable as Singapore would only rely on a single method to guard her national interests and sovereignty. In the event of a war or conflict and the SAF is called upon to utilise its conventional war fighting skill set, the ramifications on Singapore's economy and population would be far reaching. Unlike other geographically larger countries where parts of the country are able to function normally despite an ongoing war, Singapore's lack of strategic depth means that the whole country will be affected—the economy will grind to a halt and almost half the population will be mobilised for the war effort. Singapore might win the war, but damage to Singaporean's way of life would take generations to recover. It is highly doubtful that any Singaporean would support such a strategy. Given the drastic consequences and the difficulty of recovery in a war scenario, it would be in our interests to avoid getting into war as far as possible. In the name of 'prevention is better than cure', it would make sense to build up layers of buffers via deterrence and diplomacy.

As much as we devote our efforts to prevent a war scenario, we cannot entirely eliminate the possibility of war. We still need to be prepared for that non-zero probability of a war scenario. Moreover, it is not feasible for the SAF just to focus on either coalition operations or OOTW and forgo the conventional war fighting skill set. As argued earlier, the ability to ensure a victory in any conflict is the bread and butter of any armed forces in the world. If the SAF loses this ability, the SAF will be merely an empty shell, trying to achieve deterrence or diplomacy without any real substance. If the SAF chooses this scenario, potential adversaries, even those with rudimentary intelligence gathering capability, will notice that the SAF's deterrence and diplomacy is not premised on something concrete and substantial. The strategy of forgoing the SAF's conventional war fighting skill set would be bound to fail.

THE RESOURCE CHALLENGE

Every year, MINDEF gets a significant portion of the Singapore Budget. MINDEF was allocated S$12.08 billion in FY2011 and S$12.3 billion in FY2012, approximately a quarter of the government's annual expenditure, towards achieving its mission.[16] While the MINDEF budget is capped at 6% of the national gross domestic product (GDP), the MINDEF budget

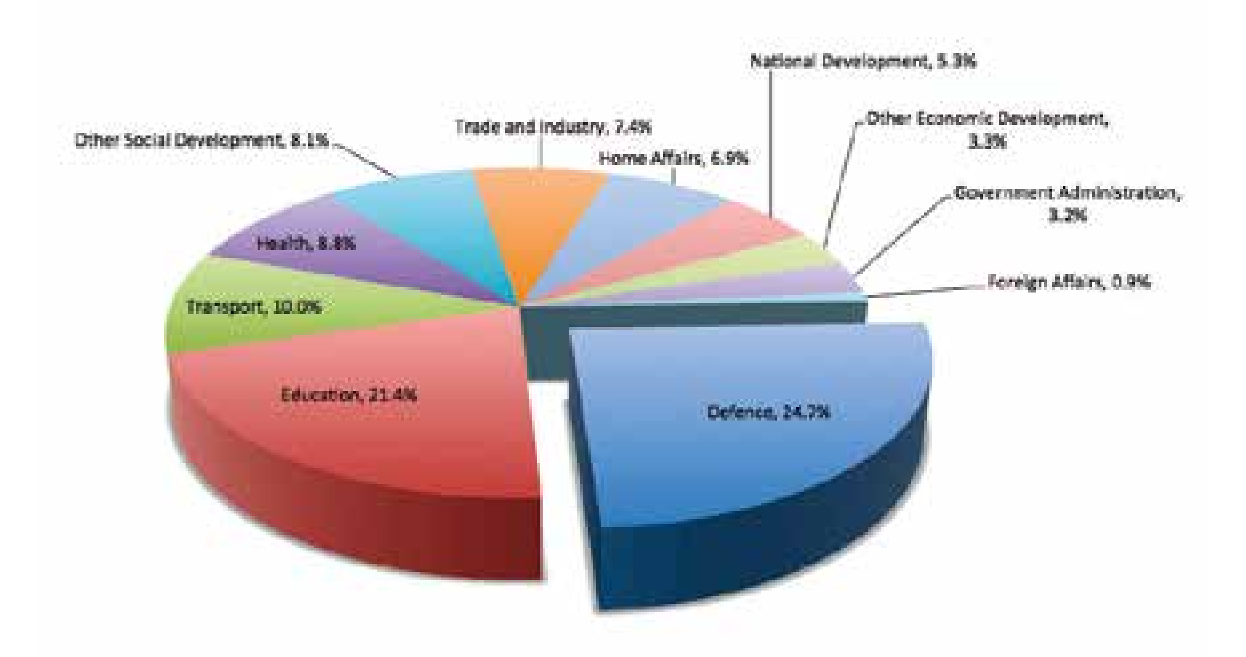


Figure 4: Percentage of Government Expenditure in FY2011.[15]

since 2002 had typically been between 4.5% and 5% of the GDP, growing by about 4% annually on average.[17] The steady defence budget over the years, through both good and difficult economic times, sends a strong signal of Singapore's commitment to defence and ensures that the SAF is always well prepared to confront security challenges.

Over the last couple of years, there have been calls for a moderation in MINDEF's share of the annual budget. During the 2012 Committee of Supply Debate in Parliament, Mr. Pritnam Singh who is a Workers Party Member of Parliament (MP) for Aljunied Group Representation Constituency (GRC), brought up the possibility for some of MINDEF's budget to be spent on social security instead:

> *"… the security architecture in the region, in particular Association of Southeast Asian Nations (ASEAN), and the relationship between the militaries in the region gives reason to be relatively positive about the low probability of outright military conflict breaking out in the region. This is especially in view of the national resources expended towards defence diplomacy in particular… the paradigm that defines the strategic environment, especially between our immediate neighbours appears to be entering a new phase of stability. This will inevitably increase the pressure on the government to reduce the defence budget for uses, such as health and education."*[19]

There is an increasing perception by members of the Singaporean public that Singapore is in no danger of being attacked by a foreign aggressor. In addition to Mr. Pritnam Singh's comment in Parliament, the discussions on various online blogs and forums have echoed a growing sentiment that the MINDEF budget should be reduced. Given Singapore's ageing population, it is understandable that there will be growing pressures for more expenditure to be allocated towards social spending. The Ministry of Health, for example, would require a higher expenditure as Singapore strives to keep healthcare affordable for the growing number of elderly Singaporeans.[20]

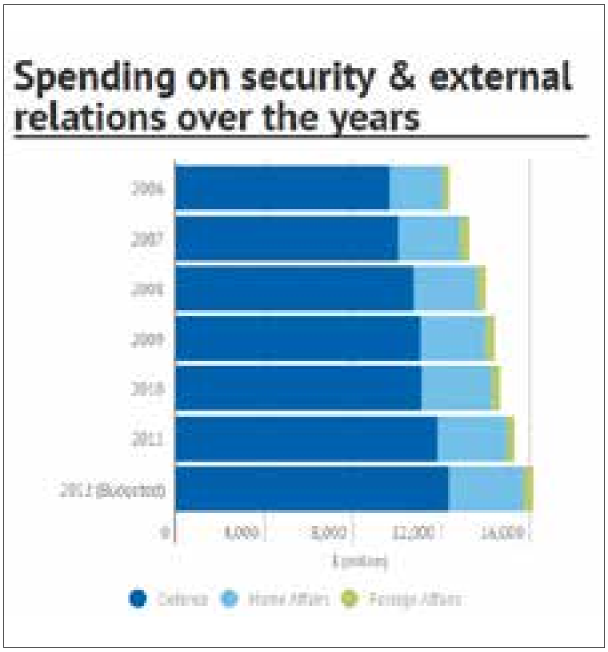


Figure 5: Spending on Defence since 2006.[18]

For full spectrum operations to continue to remain a viable strategic posture for the SAF, there has to be sufficient resources for MINDEF to undertake efforts in all three military operational skill sets. The competition for a slice of the Singapore Budget will undoubtedly place pressures on MINDEF in the coming years. The commonly held perception is that militaries around the world are reducing their budgets and Singapore should do the same, especially with favourable regional atmospherics. In 2011, 62 countries reported a decrease in military spending due to austerity and deficit-reduction measures in the wake of the global financial and economic crisis that broke in 2008.[22] 18 European countries have seen

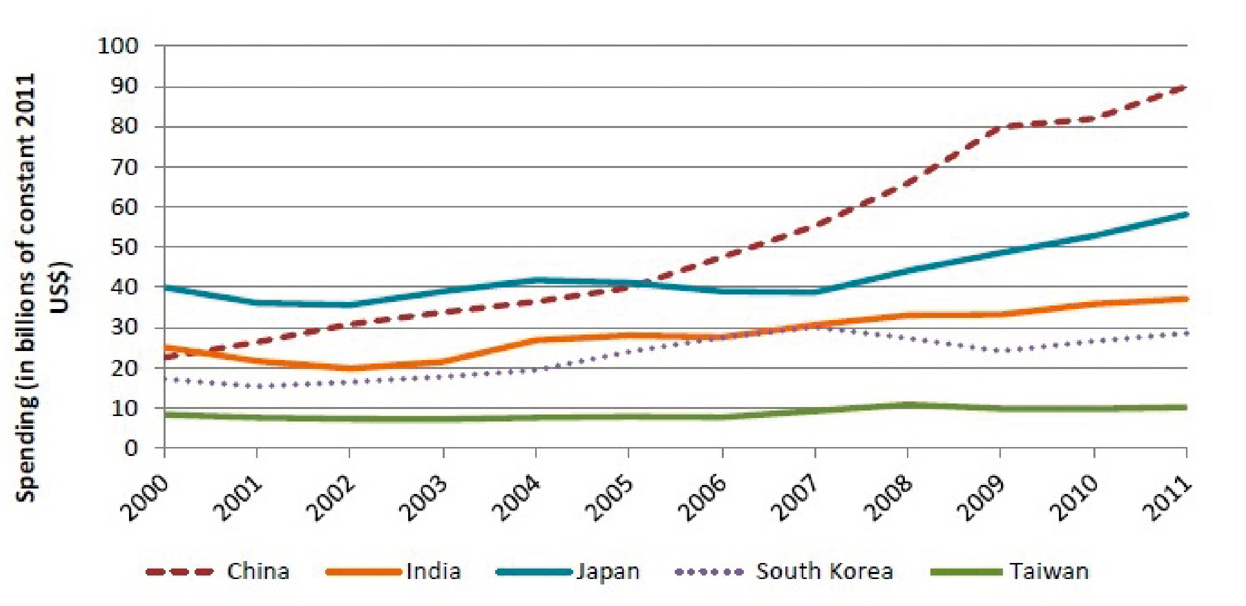


Figure 6: Growth in Defence Spending since 2000.[21]

real-terms falls of more than 10% in military spending since 2008.[23] Even the largest two spenders in Europe, the United Kingdom (UK) and Germany, plan further cuts of at least 7.5% through till 2015.[24]

For MINDEF and the SAF to ensure that full spectrum operations continue to be a viable strategic posture for the SAF, the SAF has to both enhance its public trust, as well as to learn to increase efficiency to do more with less.

This common perception is inaccurate as the major countries in Asia have been increasing their defence spending over the past five years, even during the economic downturn. This trend is unlike to change especially with the various territorial disputes, such as the Spratly Islands and Diaoyu Islands, in the region.

Singapore's defence expenditure, apart from allowing the SAF to ensure mission success, also has a huge signaling effect on the defence watchers as well as countries in the region. MINDEF's annual budget allocation is a publicly available number and a downward trend to the budget may give the impression that Singapore is changing her attitude towards the defence of the nation. In the medium to long term, this impression will make us potentially more vulnerable.

For MINDEF and the SAF to ensure that full spectrum operations continue to be a viable strategic posture for the SAF, the SAF has to both enhance its public trust, as well as to learn to increase efficiency to do more with less.

The public trust in the SAF spending its budget prudently is essential for the SAF to maintain full spectrum operations. If this public trust was lost, it would be difficult for the government, regardless of the political will, to allocate MINDEF and the SAF with a sufficient budget to maintain full spectrum operations and to achieve its mission. Minister for Defence, Dr Ng Eng Hen, has also reiterated this in the 2012 Committee of Supply debate.[25]

It is also possible that in the coming years, the budget allocated to MINDEF will be reduced in either real or absolute terms. The MINDEF portion of the budget may also be capped at the lower value than the current 6%. MINDEF and the SAF would have to increase the efficiency of the allocated budget to achieve its mission. Through creativity, innovation and education, the SAF can refine its processes and doctrines to reap a greater return on each defence dollar spent. New training pedagogies can also be explored to ensure that SAF personnel remains well trained and "prepared for a wider spectrum of operations to operate with other national security and civil agencies, with coalition partners, with NGOs in the glare of the global media."[26]

CONCLUSION

For the MINDEF and the SAF to achieve its mission, it is a necessity for the SAF to maintain the strategic posture of full spectrum operations. Electing to choose and focus on just one of the military operational skill set would be foolhardy and ultimately disastrous for Singapore, especially in times of need. The ability for the SAF to maintain full spectrum operations in the future would depend on the resources available to MINDEF. In the near future, the budget allocated to MINDEF will inevitably face increasing pressures from social development sectors. MINDEF and the SAF will need to continue to build on the public trust and to be prudent in the spending of the tax dollar. In addition, there will be an increasing need for the SAF to find ways to reap a greater return on each defence dollar spent.

REFERENCES

Alexander, Keith. "U.S. Cyber Command: Organizing For Cyberspace Operations, Statement Before The House Committee On Armed Services,"

Andrew Krepinevich. Cyber Warfare – A "Nuclear Option"?. Center for Strategic and Budgetary Assessments. 25.

Ball, James. The Washington Post, "Iran preparing internal version of Internet." 2013. http://articles.washingtonpost.com/2012-09-19/world/35496978_1_huawei-iranian-activists-iranian-government.

Chico, Harlan, and Ellen Nakashima. "Suspected North Korean cyberattack on a bank raises fears for S. Korea, allies." The Washington Post, August 29, 2011. http://articles.washingtonpost.com/2011-08-29/world/35271097_1_bank-incident-bank-attack-cyberattack (accessed December 24, 2012).

Chong, Alan, and Liang Tuang Nah. S Rajaratnam School Of International Studies, "Framing Cyber Warfare: Between Offence and Defence." 2013. http://www.rsis.edu.sg/publications/Perspective /RSIS0952011.pdf.

Clarke, Richard. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins Publishers, 2010.

Cordon, Gavin. "Armed forces are vulnerable to cyber attack, warn MPs." The Independent, 2013. http://www.independent.co.uk/news/uk/home-news/armed-forces-are-vulnerable-to-cyber-attack-warn-mps-8443693.html (accessed January 12, 2013).

Dorothy, Denning. "Barriers to Entry," IO Journal (2009): 6-10, http://faculty.nps.edu/ dedennin/publications/Denning-BarriersToEntry.pdf

Derrick, Ho. The Straits Times, "An interactive look at how the Government has spent its money over the years." 2013. http://www.straitstimes.com/the-big-story/budget-2013/story/interactive-look-how-the-government-has-spent-its-money-over-the-yea.

Ellen, Nakashima. The Washington Post, "Stuxnet was work of U.S. and Israeli experts, officials say." 2013. http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials.

Eneken, Tikk, Kaska Kadri, Rünnimeri Kristel, Kert Mari, Talihärm Anna-Maria , and Vihul Liis. NATO Cooperative Cyber Defense Centre of Excellence , "Cyber Attacks Against Georgia: Legal Lessons Identified." 2013. http://www.carlisle.army.mil/ DIME/documents/Georgia 1 0.pdf.

Fildes, Jonathan. BBC, "Stuxnet virus targets and spread revealed." 2013. http://www.bbc.co.uk/news/technology-12465688.

Gargan, John. "To Defend a Nation: An Overview of Downsizing and the U.S. Military." M@n@gement. 2. no. 3 (1999): 221-232. http://www.management-aims.com/PapersMgmt/23Gargan.pdf

Jeffery Carr. Inside Cyber Warfare: Mapping the Cyber Underworld, (Sebastopol: Oreilly Media, 2011).

Kaspersky Lab, "Kaspersky Lab provides its insights on Stuxnet worm." 2013. http://www.kaspersky.com/about/news/ virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm.

Krepinevich, Andrew. Center for Strategic and Budgetary Assessments (CSBA), "Cyber Warfare: A “Nuclear Option”?." 2012.

Lim, Richard. "Operation Blue Sapphire - Reflections." POINTER. v._36. n._2 (2010): 23-29. http://www.mindef.gov.sg/content/imindef/publications/pointer/journals/2010/v36n2/feature4/_jcr_content/imindefPars/0003/file.res/23-29_Operation_Blue_Sapphire lowres.pdf

Limer, Eric. Gizmodo, "Meet Red October: The Global Cyber-Espionage Ring That Spent 5 Years in the Shadows." 2013. http://gizmodo.com/5975793/meet-red-october-the-global-cyberespionage-ring-that-spent-5-years-in-the-shadows.

LiveSquare Security, "Cyber Warfare: the good, the bad, the ugly." 2012. http://www.arizonatele.com/atic/docs/ ATIC_Cyber_Warfare_Presentation_11_17_11.pdf.

Lynn, William. US Department of Defense, "Defending a New Domain : The Pentagon's Cyberstrategy." 2012. http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx.

Mann, Joseph. Fatal System Error. New York: Public Affairs, 2010.

Markoff, John. "Old Trick Threatens the Newest Weapons." The New York Times, 2009. http://www.nytimes.com/2009/10/27/science/27trojan.html?ref=cyberwar &_r=0.

Markoff, John, and Andrew Kramer. "U.S. and Russia Differ on a Treaty for Cyberspace ." The New York Times, 2009. http://www.nytimes.com/2009/06/28/ world/28cyber.html?pagewanted=all

Ministry of Home Affairs, "1 October 2009: Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats." 2013. http://www.mha.gov.sg/ news_details.aspx?nid=MTU2MQ==-OtPkaml9VAY=.

Netmarketshare.com, "Desktop Operating System Market Share." 2013. http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0.

Netmarketshare.com, "Mobile/Tablet Operating System Market Share." 2013. http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1.

Paganini, Pierluigi. "Concerns Mount over North Korean Cyber Warfare Capabilities." 2012. http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html (2012).

Posner, Gerald. The Daily Beast, "China's Secret Cyberterrorism." 2012. http://www.thedailybeast.com/articles/2010/01/13/chinas-secret-cyber-terrorism.html

Public Broadcasting Service, "The Uses of Military Power." 2013.
http://www.pbs.org/wgbh/pages/frontline/ shows/military/force/weinberger.html.

Ramesh, S. "New IT Security Authority to safeguard Singapore against cyber threats." Channel News Asia, 2009.
http://www.channelnewsasia.com/stories/singaporelocalnews/print/1008285/1/.html.

Reed, John. DefenseTech, "Proof That Military Chips From China Are Infected?." 2012. http://defensetech.org/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected/.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends ." Virtual Battlefield.
http://www.ccdcoe.org/publications/virtualbattlefield/01_SHARMA_Cyber_Wars.pdf (2013).

The Economist, "Cyberwar: War in the fifth domain." 2013.
http://www.economist.com/node/16478792.

Thomas C. Reed, At the Abyss: An Insider’s History of the Cold War (New York, 2004).

UPI. "North Korea blamed for cyberattack." 2011. http://www.upi.com/ Top_News/World-News/2011/08/30/North-Korea-blamed-for-cyberattack/UPI-48281314 705600/ (2012).

ENDNOTES

1. *MINDEF*, "Speech by Mr. Teo Chee Hean, *Minister for Defence*, at SAFTI MI 10th Anniversary Dinner, 25 August 2005." http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2005/aug/25aug05_nr2/25aug05_speech2.print.img.html.

2. *MINDEF*. SAF Mission. http://www.mindef.gov.sg/imindef/about_us/mission.html

3. Huth, Paul. "Deterrence And International Conflict: Empirical Findings and Theoretical Debates." *Annual Review of Political Science*. 2. (1999): 30.

4. Codner, Michael. Royal United Services Institute, "Defining '*Deterrence*' - Framing Deterrence in the 21st Century." http://www.rusi.org/downloads/assets/Defining_Deterrence_-_A_Pre-Conference_Note.pdf.

5. *MINDEF*, "Speech by Minister for Defence Dr Ng Eng Hen, at the Overseas Service Medal Presentation Ceremony." 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2011/30jun11_speech.print.img.html.

6. Medcalf, Rory. The Diplomat, "Can Military Diplomacy Keep the Peace in 2013?." 2013. http://thediplomat.com/flashpoints-blog/2013/01/05/can-military-diplomacy-keep-the-peace-in-2013/.

7. Muthanna, KA. "Military Diplomacy." *Journal of Defence Studies*. 5. no. 1 (2011): 3. http://idsa.in/system/files/jds_5_1_kamuthanna.pdf 2013.

8. S.Rajaratnam School of International Studies (RSIS), "DEFENCE DIPLOMACY IN SOUTHEAST ASIA."2013. http://www.rsis.edu.sg/publications/conference_reports/Defence Diplo book.pdf.

9. Lim, Richard. "Operation Blue Sapphire - Reflections."*Pointer*. v._36. n._2 (2010): 23-29. http://www.mindef.gov.sg/content/imindef/publications/pointer/journals/2010/v36n2/feature4/_jcr_content/imindefPars/0003/file.res/23-29_Operation_Blue_Sapphire lowres.pdf (2013).

10. Ibid. 4.

11. *MINDEF*, "Speech by Minister for Defence Dr Ng Eng Hen, at the Overseas Service Medal Presentation Ceremony (2011)." 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2011/nov/18nov11_nr2/18nov11_speech.print.img.html.

12. Gargan, John. "To Defend a Nation: An Overview of Downsizing and the U.S. military." M@n@gement. v._2. n._3 (1999): 221-232. 2013. http://www.management-aims.com/PapersMgmt/23Gargan.pdf

13. Public Broadcasting Service, "The Uses of Military Power." 2013. http://www.pbs.org/wgbh/pages/frontline/shows/military/force/weinberger.html.

14. Wei Chong, Ong. S.Rajaratnam *School of International Studies*, "Singapore's Defence Spending: A Long-term Approach." 1. 2013. http://www.rsis.edu.sg/publications/Perspective/RSIS0062010.pdf.

15. *Ministry of Finance*, "Singapore Budget FY2011 Expenditure Estimates." 2013. http://www.mof.gov.sg/budget_2011/revenue_expenditure/attachment/5GOS Expenditure EE2011.pdf.

16. *Ministry of Finance*, "Singapore Budget 2012." 2013. http://www.mof.gov.sg/budget_2012/expenditure_overview/mindef.html.

17. Channel News Asia, "MINDEF manages its budget "prudently": Ng Eng Hen." 2013. http://www.channelnewsasia.com/stories/singaporelocalnews/view/1187342/1/.html.

    MINDEF, "Speech by Minister for Defence Teo Chee Hean, at Committee of Supply Debate 2009." 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/ps/2009/12feb09_ps/12feb09_ps3.print.img.html.

    MINDEF, "Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2012." 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/ps/2012/06mar12_ps/06mar12_ps.print.img.html.

18. Derrick, Ho. *The Straits Times*, "An interactive look at how the Government has spent its money over the years." 2013. http://www.straitstimes.com/the-big-story/budget-2013/story/interactive-look-how-the-government-has-spent-its-money-over-the-yea.

19. Singh, Pritnam. *MINDEF*, "Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2012." Last modified 06 Mar 2012. Accessed February 4, 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/ps/2012/06mar12_ps/06mar12_ps.print.img.html.

20. *Ministry of Finance*, "MINISTRY OF HEALTH (MOH)." 2013. http://www.mof.gov.sg/budget_2012/expenditure_overview/moh.html.

21. Center for Strategic and International Studies, "Asian Defense Spending, 2000-2011." 2013. http://csis.org/files/publication/121005_Berteau_AsianDefenseSpending_Web.pdf.

22. Stockholm International Peace Research Institute, "Recent trends in military expenditure." 2013. http://www.sipri.org/research/armaments/milex/resultoutput/trends.

23. Ibid.

24. Ibid.

25. Ibid, 6.

26. *MINDEF*, "Speech by Mr. Teo Chee Hean, Minister for Defence, at SAFTI MI 10th Anniversary Dinner, 25 August 2005." 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2005/aug/25aug05_nr2/25aug05_speech2.print.img.html.

MAJ Lee Hsiang Wei is a Helicopter pilot by vocation and is currently Officer Commanding, 126 SQN, Helicopter Group. MAJ Lee was a recipient of the SAF Overseas Scholarship in 2004 and he graduated from Cornell University with a Bachelors of Science in Electrical and Computer Engineering and a Masters of Engineering. MAJ Lee also won the 2nd Prize in the 2012/2013 and 2014/2015 Chief of Defence Force Essay Competition.

Cyber Attacks and the Roles the Military Can Play to Support the National Cyber Security Efforts

by **ME5 Alan Ho Wei Seng**

Abstract:

The advent of low cost computing devices and fast access to the Internet has brought forth great convenience to everyday life, but there are also many cyber threats lurking in cyberspace, waiting to exploit system or network vulnerabilities so as to compromise their integrity, availability, and confidentiality. On a national level, cyber attacks can exploit the vulnerabilities of critical infrastructures such as the energy, transportation and communications sectors and seriously undermine military mission success, since the infrastructures are critical in supporting the conduct of military operations. Therefore, there is vested interest for the military to partner with other defence agencies, private sectors and possibly international players to enable a 'whole-of-nation' effort to develop comprehensive cyber security measures in order to mitigate the impact of cyber attacks. This is essential as cyberspace may eventually be commonly accepted as a military domain of conflict.

Keywords: Internet; Cyber Attacks; Compromise; Exploit Vulnerabilities; Vested Interest

INTRODUCTION

> *"We have to consider (cyber security threats) every bit as foundational as we do in our ability to manoeuvre forces as a military construct."*
>
> *- US Navy Admiral Michael S. Rogers*
> *Commander of US Cyber Command*
> *Director of the National Security Agency*
> *Chief of the Central Security Service*[1]

In this Information Age, the technological advancements of the Internet have enabled information to be more accessible to much of the world population, and at an increasing speed.[2] Based on data retrieved from 'Worldometers', the world population stands at 7.2 billion as of end 2014, of which 3 billion or close to 50% of the populace have access to the Internet.[3] As Internet usage continues to expand, cyberspace, which is the national environment that communication over computer networks occurs, will become increasingly woven into the fabric of everyday life across the globe.[4] Hopping onto the cyberspace bandwagon, militaries around the world, like the United States (US), have harnessed onto the good prospects offered to better conduct its operations: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations.[5]

However, we need to be cognisant of this reliance on cyberspace as there are many system or network vulnerabilities, which are weaknesses that allow an attacker to compromise the integrity, availability and confidentiality of the system or network used.[6] Cyber attacks can exploit these vulnerabilities and penetrate the computers or networks of a user, company or even nation, for the purpose of causing damage or disruption.[7] One recent cyber attack incident was what US President Barack Obama termed as an act of 'cyber vandalism': in December 2014, Sony Pictures broadcasted a movie depicting the assassination of the North Korean leader, Kim Jong-un.[8] On a national level, cyber attacks on critical infrastructures such as the energy, transportation and communications sectors could seriously undermine military mission success since the infrastructures are critical in supporting the conduct of military operations.

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT Y
NEIGHBOURS AND THIS IS THE END
SETH ROGEN JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시
THE
INTERVIEW
인터뷰
Wikipedia

Movie poster of 'The Interview', which depicted the assassination of North Korean Leader, Kim Jong-un.

Therefore, there is vested interest for the military to participate in the national effort to develop comprehensive cyber security measures, which could include the legislation of governing policies, implementation of cyber security tools and best practices, as well as the training of appropriate cyber security experts to better safeguard the organisation and user's assets.[9] The importance of cyber security was echoed in the private sectors through an Information Assurance (IA) survey conducted in 2014, of which 75% of respondents named cyber security and privacy as primary concerns.[10] In Singapore, the government is stepping up efforts to strengthen the nation's resilience towards cyber attacks. In order to complement the existing national cyber security efforts, it was reported in 2014 that a new Cyber Security Research Centre will be set up to study and develop capabilities in cyber forensics and mobile security.[11] For the Singapore Armed Forces (SAF), it was reported in 2013 that a new hub has been set up to consolidate its cyber security experts to monitor cyber threats round the clock and muster a sharper response to thwart cyber attacks and digital spies.[12] Cyber security is also gaining traction academically. For example, Nanyang Polytechnic has collaborated with the Centre for Strategic Infocomm Technologies (CSIT) to offer bond-free scholarships to qualified students who enroll into their Diploma in Cyber Security and Forensics.[13]

In summary, this essay looks at the attributes and techniques employed in cyber attacks. It also articulates the impact of cyber attacks on the military, and roles the military can play to support the national cyber security efforts in mitigating the impact of cyber attacks so as to safeguard the nation's cyber well-being.

ATTRIBUTES OF CYBER ATTACK

Cyber Attacks are Asymmetric

With the advent of low cost computing devices, cyber attackers can exert an adverse impact disproportionate to their size. They do not require sophisticated weaponry, and neither do they have to build expensive platforms such as stealth fighters or aircraft carriers, in order to compromise the network of interest and pose a significant threat.[14] Besides state actors, there are concerns that terrorists or organised criminal groups could stage cyber attacks that leverage on the low capital outlay required. For instance, it was reported in 2009 that Iraqi insurgents had utilised software available for only US$26 to hack into video imagery relayed by a US drone aircraft, thus allowing them to see what the US military was seeing.[15]

Offense has the Advantage and Speed

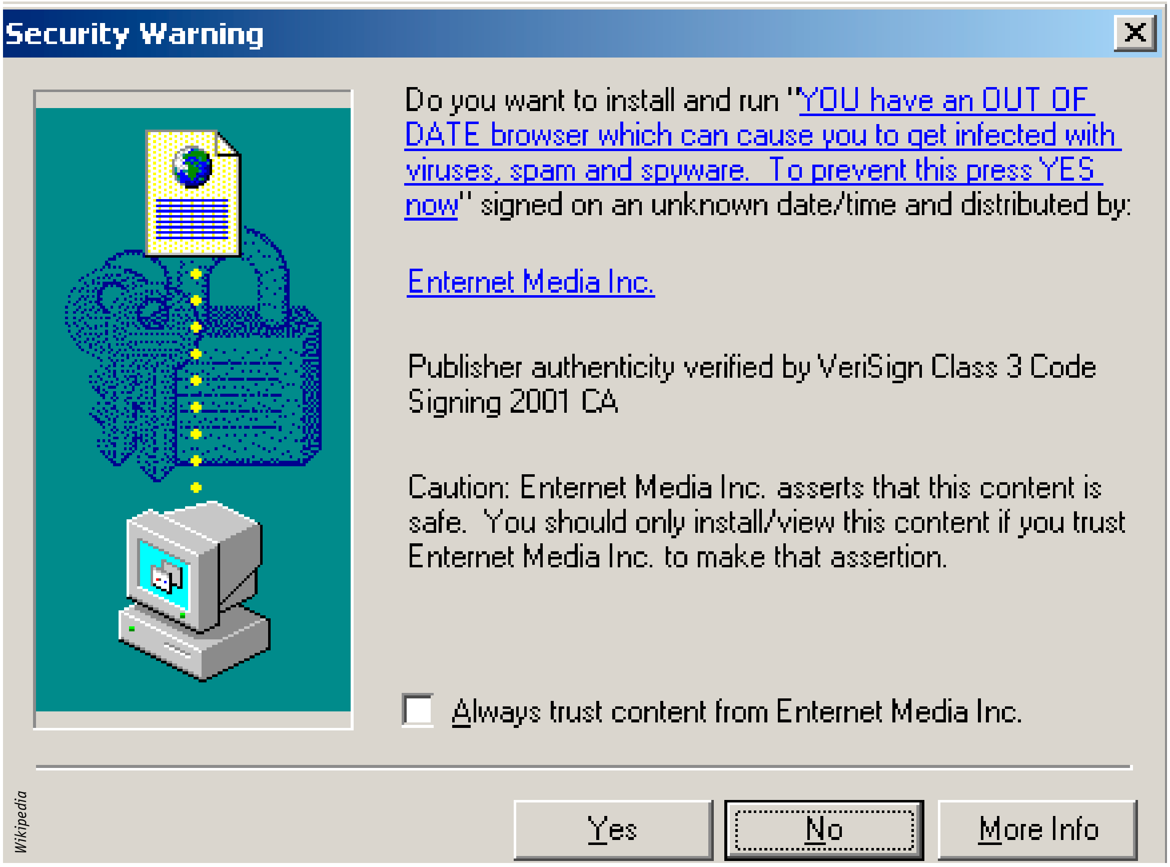
Cyber attacks are like manoeuvring forces where speed and agility matter most, and offense can have the upper hand in an instance. A fortress mentality will not work in an offense-dominant cyberspace environment since there is little to retreat to behind a Maginot Line of firewalls or the user will risk being overrun.[16] Offense has the advantage over defence because the defender must contend with millions of lines of codes, while the attacker only has to find a single vulnerability to quickly destabilise the situation, which is possible to unfold in a few minutes. This is as opposed to conventional warfare, where it would take from, at the very least, minutes to a few hours to carry out, as missiles are fired at targets or aircraft, tanks, and ships are sent into battle.

The ability of cyber attacks to reach the desired targets without the need for mass deployment of troops, delivery vehicles or weapons, or foreign bases, coupled with its sheer velocity represents a new dimension to warfare that could dramatically increase the need for immediate and possibly risky decision-making by governments under attack.[17] Former US Secretary of Defense Leon Panetta previously commented on the reaction of US to cyber attack, that "the US may consider preemptive strikes if it detects imminent threat of an attack that will cause a significant physical destruction in the US or kill American citizens."[18] To stay ahead, it is imperative to constantly adjust and improve cyber security measures.

With the advent of low cost computing devices, cyber attackers can exert an adverse impact disproportionate to their size. They do not require sophisticated weaponry, and neither do they have to build expensive platforms such as stealth fighters or aircraft carriers, in order to compromise the network of interest and pose a significant threat.

Difficult to Detect and Attribute

It is hard to deter if you cannot punish, and you cannot punish without first knowing who is behind an attack. For the military, the traditional deterrence model of assured retaliation when attacked will be difficult to execute in cyberspace because it will be challenging to identify the ownership of an attack accurately.[19] This is because a missile will likely come with a distinct signature, but the same cannot be said for a computer virus if the digital footprints are well-covered. Furthermore, the preparations for cyber attack are far less visible than that for conventional warfare. For the latter, preparations are usually evident through a military build-up and mobilisation order which are easily detectable, but there are no visible signs of preparations when it comes to cyber attacks.[20] Even so, if there was a heavily masked attack employing dynamic proxies and routing that spans across many countries where jurisdiction over cyber security could differ or be lacking, it could potentially compound the inability to attribute an attack swiftly, let alone obtaining its intent.



Security Warning

Do you want to install and run "YOU have an OUT OF DATE browser which can cause you to get infected with viruses, spam and spyware. To prevent this press YES now" signed on an unknown date/time and distributed by:

Enternet Media Inc.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA

Caution: Enternet Media Inc. asserts that this content is safe. You should only install/view this content if you trust Enternet Media Inc. to make that assertion.

□ Always trust content from Enternet Media Inc.

A malicious website trying to install spyware on readers' computers in the past. The technology to do so today is much more sophisticated.

Even in a fortunate case whereby an attack could be attributed to the attacker, if it is a non-state actor, such as a terrorist group, it may not have any assets against which the nation can retaliate. To gain easier access and evade detection, attackers can also target defense contractors and subcontractors, whose networks tend to be less secured than the military which they are supporting.[21] These attacks often rely on socially engineered emails, or 'spear phishing', which are made to look authentic to the recipient, and when opened will install a remote-access tool for the attacker.[22] This heightens the necessity to protect the computer network of defence contractors and subcontractors, indirectly offering better protection for the military which they are supporting. One way to mitigate this could be to ensure that the attacks are fruitless by developing resilient systems that are able to withstand serious technical compromises and adapt to changing their Standard Operating Procedures (SOPs) when required, instead of investing resources to find the source to inflict a direct penalty on the attackers, which could potentially be a dead-end.[23]

TECHNIQUES OF CYBER ATTACK AND THEIR IMPACT TO THE MILITARY

Underpinned by the wealth of information available on cyberspace and low cost computing devices, cyber attackers are becoming more tech-savvy and able to launch sophisticated intrusions into the networks that control the national infrastructures. One such intrusion is the Distributed Denial of Service (DDOS) that floods the systems (of

Cyberwar Defense team of the US Air Force monitoring cyber threats at a workstation.

the national infrastructures) with multiple requests, more than they could respond to and paralysing them consequently. DDOS is usually executed by 'botnets' comprising networks of computers that have been hijacked by remote users, often without the owner's knowledge.[24] Other than networks, software and hardware are also at risk of being tampered with even before they are linked together in an operational system. 'Logic bombs' are rogue software programming codes that can cause sudden malfunctions when developed, while hardware can have 'kill switches' and hidden 'back doors' written into the computer chips that allow remote-access by unintended users.[25] Computer-induced failures of national infrastructures could cause massive physical damage and economic disruption. The military strength of a nation ultimately depends on her economic vitality, so cyber vulnerabilities could erode both the nation's military effectiveness and its competitiveness in the global economy, if the attacks are pervasive and persistent.

Cyber security is a discipline that requires national effort, and it is not something that the citizens and private companies can expect to outsource to the military.

On the impact of cyber attacks to the military, the exploitation of vulnerabilities in military cyber systems could result in weapons blueprint, operational plans and surveillance data being compromised, which could seriously undermine national security. For instance, a rogue programme that was introduced by an infected flash drive inserted into a US military laptop at a Middle East base was able to gain access to information within networks operated by the US Central Command.[26] Cyber attack techniques that can infiltrate military systems can be made stealthy to ensure that rogue programmes, when introduced, remain undetected. They could establish a digital 'beachhead' from which these programmes operate silently to stealthily exfiltrate sensitive military operational plans to unintended servers under foreign control. Noting the gravity of a cyber attack, the US has asserted the belief that such an attack could be regarded as an act of war, and that the US could respond using traditional military force.[27]

THE ROLES THE MILITARY CAN PLAY TO SUPPORT THE NATIONAL CYBER SECURITY EFFORTS

Cyber security is a discipline that requires national effort, and it is not something that the citizens and private companies can expect to outsource to the military. Any nation that depends heavily on the military for cyber security will reduce the incentives for the private sector, especially Multinational Corporations (MNCs) who possess adequate resources for the necessary Research and Development (R&D), to develop cyber wellness provision.[28] Furthermore, few private sectors are likely to welcome hands-on assistance from the military since the former would be better poised to defend their own networks, business data privacy concerns aside.[29]

Therefore, a partnership is one position which the military can consider—collaborating with other government departments/agencies, and the private sector (including defence contractors) to enable a 'whole-of-nation' cyber security strategy, albeit there is still the lingering question for a neat way to rationally and effectively divide the national cyber security responsibilities between the military, and the rest.[30] The following are four initiatives in which the military can play such supportive roles, collectively working as a team with other defence agencies, private sectors and possibly international players.

Cyber Security Governance and Practices

The teams can collaborate and enact policies to govern cyber security through standardising operating procedures in cyberspace so as to better protect classified networks which could house sensitive information and enable crucial war-fighting, diplomatic, counter terrorism, law enforcement, intelligence and homeland security operations. The sharing of best practices for cyber security amongst the team members can provide operational norms to deal with cyber threats and incident responses, especially those that could cause exceptionally grave damage to the national security. The developed cyber security governance and practices must be enduring against the fast-paced cyberspace, and aimed at building an approach to cyber defence strategy that deter interference and attack in cyberspace. The cyber defence strategy can be further enhanced by improving warning capabilities, articulating roles for private sector and international players, and developing appropriate responses for both state and non-state actors.[31]

Since the nation depends on a variety of privately owned and operated critical infrastructures to carry out the public's businesses, the team can help define its role by advocating and extending cyber security governance and practices into the critical infrastructures domains. In the US, there is existing and ongoing partnership between the Federal Government, the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR) in addressing security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities.[32] It also includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR.[33]

Cyber Threat Research and Warning

It is essential to know the current state of play in cyber threats in order to develop appropriate cyber security governance and policies to address them. Similar to mapping the threat landscape of a military adversary, the team can collaborate in researching emerging cyber threats and developing measures/technologies to forewarn imminent cyber attacks. This involves mapping the entire cyber landscape that the nation is operating in, establishing a healthy baseline of cyber well-being, and determining the threshold in which, when that baseline is crossed, it could indicate a possible cyber attack. In addition, the team can research and provide an understanding to the relationship between recovery time and value of a cyber attack, assuming an attacker is less motivated to take down a network, if the victim can quickly restore it to operation.[34]

Also, against the fast-paced cyber threat landscape, it is imperative for cyber security experts to keep abreast of the adversary, if not at least staying alongside, through continuous learning and regular currency checks, to help shape an open, vibrant and stable cyberspace, which the public can use safely.

The cyber threat research is contingent on a robust relationship with internal defence agencies, private sectors and also international players to share intelligence on threat signatures/actors, analytic and collaborative technologies in order to maximise the advantage of each organisation's unique capabilities and provide timely and accurate assessments to support the nation's decision makers. For instance, the National Cyber Security Center (NCSC) within the Department of Homeland Security plays a key role in securing US Government networks and systems by co-ordinating and integrating information from all relevant agencies to provide cross-domain situational awareness, analysing and reporting on the state of US networks and systems, and fostering inter-agency collaboration and coordination.[35] It is unlikely for a single entity to be aware of the overall nation's cyber security efforts, so the team can also help to co-ordinate the nation's R&D in cyber security and redirect efforts to where they are needed. This initiative is critical in eliminating redundancies, identifying research gaps and prioritising R&D efforts, in order to justify the usage of public money in strengthening the nation's cyber well-being.

Cyber Security Measures and Implementation

In the military, war gaming is rudimentary in developing nascent operation concepts and processes, since they can be clinically tested without massive resources, as compared to the actual maneuvering of forces. One possible cyber security measure and implementation is in developing a Cyber Range/Simulation system to enable the development and testing of cyber tools, best practices, policies for robustness in core system architecture. This could force the redesign or retrofit of hardware, Operating System (OS), and computer languages with cyber security in mind, and the same set of consideration should also be extended to the systems of defence contractors to build unified cyber security architectures.[36] The military could lend their war gaming experiences and facilities to simulate how technical systems might respond to various attacks and provocations, how cyber attacks could escalate out of control, and lastly, which games of co-operation might best thwart attacks.[37] All these can be done within the safe confines of the war gaming centres.

One such facility is the National Cyber Range that was developed by the US Department of Defense (DOD) in 2012 to allow co-operation with other US government agencies, and potentially non-US government partners to rapidly create numerous models of network, intended to enable the military and others to simulate cyberspace operations and test new technologies and capabilities, promoting collaboration and critical info sharing, in support of the 'whole-of-nation' effort.[38] One possible simulation could be studying the 'lethal radius' of a cyber weapon. Every bomb has a 'lethal radius', and any given target that lies outside of said radius is likely to be unharmed. This knowledge can help military planners minimise collateral damage. What, if any, is the cyber analogy of 'lethal radius' for cyber attacks?[39]

In addition, the team could consider developing a unified Intrusion Detection System (IDS) harnessing sensor across the military, the other defence agencies, and private sectors. In the US, the IDS called upon 'EINSTEIN 2', which uses passive and signature-based sensors from a vital part of the US Government network defences to identify when unauthorised users attempt to gain access to those networks. It also inspects Internet traffic entering Federal systems for unauthorised accesses and malicious content as well.[40] Most importantly, 'EINSTEIN 2' is capable of alerting the United States Computer Emergency and Readiness Team (US-CERT) in real-time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualisation of the derived data. Consequently, due to the capabilities of 'EINSTEIN 2', US-CERT analysts have a greatly improved understanding of the network environment and an increased ability to address the weaknesses and vulnerabilities in Federal network security, enhancing overall situation awareness. There are plans to develop the next generation system, dubbed the 'EINSTEIN 3', that will draw on commercial and government technologies to conduct real-time, deep packet inspection and threat-based decision-making on network traffic entering or leaving key networks, with the goal of identifying and characterising malicious network traffic so as to enhance cyber security analysis, situation awareness and security response.[41]

Cyber Security Training and Awareness

With massive capital invested on new technologies to secure the cyberspace, it is the people with the right knowledge and skills to implement those technologies that will make the difference and achieve mission success. The team can propose options to invest in human capital and collaborate with leading institutions that specialise in cyber security related fields to develop courses to train a cadre of cyber security experts to tackle the increasing cyber threat landscape. The US Federal Government aims to develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees, which will adopt a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge.[42]

Also, against the fast-paced cyber threat landscape, it is imperative for cyber security experts to keep abreast of the adversary, if not at least staying alongside, through continuous learning and regular currency checks, to help shape an open, vibrant and stable cyberspace, which the public can use safely. Separately, it is essential to proliferate basic cyber security hygiene awareness for both the cyber security work force and the population that rely on IT systems so that everyone can contribute towards a secure future for cyberspace and the users.

CONCLUSION

Cyber security includes protecting military networks against cyber threats. Cyberspace is a network of networks that includes countless computers across the globe, therefore no state or organisation can unilaterally maintain effective cyber security. Close co-operation and timely sharing of cyber events, threat signatures of malicious code, and information about emerging actors/threats, allies and international players can improve collective cyber security standards. The military should continue to explore possible ways to defend its networks from malicious threats, and invest in people, technologies and R&D to create and sustain the cyberspace capabilities that are vital to national cyber security. This is essential as cyberspace may eventually be commonly accepted as a military domain of conflict, and it will be no different to allocating resources to procure sophisticated weaponry and developing the people to better serve in the Services and the overall Armed Forces for conventional warfare.

ENDNOTES

1. "The NSA's new look at cyber security," (*Armed with Science - The Official U.S. Defense Department Science Blog*, 2014)
   http://science.dodlive.mil/2014/06/16/the-nsas-new-look-at-cybersecurity/

2. Nazli Choucri and Daniel Goldsmith, "Lost in cyberspace: Harnessing the Internet, international relations and global security", (*Bulletin of the Atomic Scientists 68*, 2012), n._2, 70-77
   http://bos.sagepub.com/lookup/doi/10.1177/0096340212438696

3. "Current world population", (*Worldometers*, 2014)
   http://www.worldometers.info/world-population/

   "Internet users in the world - distribution by world regions 2014 Q2" (*Internet World Stats*, 2014)
   http://www.internetworldstats.com/stats.htm

4. "Definition of cyberspace", *Oxford Dictionary*
   http://www.oxforddictionaries.com/us/definition/american_english/cyberspace

5. Lynn III and William J., "Defending a new domain", (*Foreign Affairs 89*, 2010), n._5, 97-108
   http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

6. "Definition of cyber vulnerability", (*Microsoft Corp*, 2014)
   http://msdn.microsoft.com/en-us/library/cc751383.aspx

7. "Global Security Outlook", (*Singapore Defence & Security Report*, 2011), n._1
   http://connection.ebscohost.com/c/articles/57525657/global-security-outlook

8. "North Korea goes offline for 10 hours", (*Today Newspaper*, 2014)

9. "Definition of cyber security", (*International Telecommunication Union* (ITU), 2014)
   http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

10. Peter Rawlings, "Survey: Cyber security tops IA compliance agenda", (*Business Source Complete*, 2014)
    http://eds.a.ebscohost.com/eds/detail/detail?sid=62058abe-4f9f-47a5-8a8a-d478465c275d%2540sessionmgr4005&vid=2&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=97337568

11. "New Cyber Security Centre to Defend Singapore's Smart Nation Systems", (*Strait Times*, 2014)
    http://www.straitstimes.com/news/singapore/more-singapore-stories/story/new-cyber-security-centre-defend-singapores-smart-nation#sthash.EgWBc8i3.dpuf

12. "SAF sets up New 'Cyber Army' to Fight Digital Threats", (*Strait Times*, 2013)
    http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630#sthash.deTt6Stu.dpuf

13. "Be a CSIT-Nanyang Scholar," (*Today Newspaper*, 2015)

14. Lynn III and William J., "Defending a new domain", (*Foreign Affairs* 89, 2010), n._5, 97-108
    http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

15. "Global Security Outlook", (*Singapore Defence & Security Report*, 2011), n._1
    http://connection.ebscohost.com/c/articles/57525657/global-security-outlook

16. Ibid., 97-108

17. Ibid., 31

18. Adam Segal, "The code not taken: China, the United States, and the future of cyber espionage", (*Bulletin of the Atomic Scientists* 69, 2013) n._5, 38-45
    http://bos.sagepub.com/lookup/doi/10.1177/0096340213501344

19. Ibid., 97-108

20. Ibid., 31

21. D. Dieterle, "Chinese hackers steal designs for top US Military Tech - Now What," (*Cyber Arms - Computer Security*, 2013) http://cyberarms.wordpress.com/2013/05/29/chinese-hackers-steal-designs-for-top-us-military-tech-now-what/

22. Ibid., 38-45

23. Alexander Klimburg, "National Cyber Security Framework Manual", (*NATO Cooperative Cyber Defence Center of Excellence*, 2014) http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

24. "The NSA's new look at cyber security," (*Armed with Science - The Official U.S. Defense Department Science Blog*, 2014) http://science.dodlive.mil/2014/06/16/the-nsas-new-look-at-cybersecurity/

25. Lynn III and William J., "Defending a new domain", (*Foreign Affairs 89*, 2010), n._5, 97-108 http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

26. Ibid., 97-108

27. Ibid., 31

28. Ian Wallace, "The Military Role in National Cyber Security Governance", (*Seoul Defense Dialogue*, 2014) http://www.brookings.edu/research/opinions/2013/12/16-military-role-national cybersecurity-governance-wallace

29. Ibid.

30. "Department of Defense Strategy for Operating in Cyberspace", (*United States of America Department of Defense*, 2011) http://www.defense.gov/news/d20110714cyber.pdf

    Thomas C. Wingfield and Robert Sharp, "Tanks in Cyberspace", (*International Policy Digest*, 2014) http://www.internationalpolicydigest.org/2014/04/14/tanks-cyberspace

31. "The Comprehensive National Cyber Security Initiative", *Executive Office of the President of the United States of America*, 2014) http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

32. Ibid.

33. Ibid.

34. Peter J. Denning and Dorothy E. Denning, "The Profession of IT - Discussing Cyber Attack", (*Communications of the ACM 53*, (2010), n._9, 29-31 http://portal.acm.org/citation.cfm?doid=1810891.1810904

35. Ibid.

36. Ibid., 97-108

37. Ibid., 29-31

38. "Department of Defense Strategy for Operating in Cyberspace", (*United States of America Department of Defense*, 2011) http://www.defense.gov/news/d20110714cyber.pdf

    "Cyber guard exercise tests people, partnerships", (*U.S. Cyber Command News Release*, 2011) http://www.defense.gov/news/newsarticle.aspx?id=122696

39. Herbert Lin, "Why computer scientists should care about cyber conflict and U.S. National Security Policy", (*Communications of the ACM 55*, (2012), n._6, 41-43 http://dl.acm.org/citation.cfm?doid=2184319.2184334

40. "The Comprehensive National Cyber Security Initiative", (*Executive Office of the President of the United States of America*, 2014) http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

41. Ibid.

42. Ibid.

ME5 Alan Ho Wei Seng is a recipient of the SAF Academic Scholarship. He graduated from the University of Queensland in 2006 with a Bachelors of Information Technology with 1st Class Honours and a Masters of Philosophy in Information Technology. In 2013, ME5 Ho received the SAF Postgraduate Award (SPA) and he graduated from Cranfield University with a Masters of Science in Forensic Computing. Following his SPA studies, ME5 Ho is presently a Deputy Branch Head. He was also a winner of the Commendation Award at the 2014/2015 Chief of Defence Force Essay Competition.

The Future of the Singapore Armed Forces Amidst the Transforming Strategic, Geopolitical and Domestic Environment

by **ME5 Gabriel Lim Guang Nian**

Abstract:

The strategic and political environment has transformed since the start of this century. The attacks on the United States on 9/11 have led to prolonged 'war against terror' campaigns in Afghanistan and Iraq with international repercussions. Within the Asia-Pacific region, heightening geopolitical rivalries between great and emerging powers have resulted in regional tensions. The role of the military in non-traditional security issues such as peacekeeping, pandemics and natural disasters has become a significant area of interest for international organisations such as the United Nations (UN), states and militaries. Domestically, we have seen greater diversity and expression of opinions on security, as well as the means to achieve it. The developments over the past 15 years have provided a glimpse into the challenges the Singapore Armed Forces (SAF) could face in the future. This essay therefore seeks to identify the future challenges facing the SAF and the means by which they may be addressed.

Keywords: Globalisation; Terrorism; Maritime Security; Humanitarian Assistance; Relevance of NS

INTRODUCTION

As a small island city-state with a lack of geographic strategic depth and little natural resources to buffer against exigencies, Singapore's approach to defence is shaped by both the unique circumstances surrounding our country's independence and the geostrategic limitations we face. To this end, Singapore has invested heavily in developing a technologically-advanced and capable military, the SAF, to defend her strategic interests and ensure her peace and security.

While the conventional threats to the city-state have not changed, the challenges facing the world—and the Asia-Pacific region in particular—mean that the SAF cannot afford to stand still. As such, to ensure that the SAF continues to be effective in its role as the defender of Singapore's sovereignty and territorial integrity, it is necessary to understand the future challenges facing the SAF and assess how the SAF can evolve to address them.

NON-TRADITIONAL TRANSNATIONAL SECURITY CHALLENGES

The increased interconnectedness brought about by globalisation has redefined the nature of security threats that countries can expect to face today. Transnational security threats of the modern era such as terrorist groups, piracy networks and the like are evolving and will continue to pose challenges to the SAF. In addition, developments in the security landscape have necessitated the SAF to progress towards a full-spectrum integrated force with capabilities to conduct Operations Other Than War (OOTW) such as Humanitarian Assistance and Disaster Relief (HADR) operations and Peace Support Operations (PSO).

Global Terrorism

The events of 9/11 in New York and Washington in 2001 demonstrated the global reach of terrorism and blurred the distinction between international and domestic security. In response to the attacks, the United States (US) led an international coalition on the Global War of Terror (GWOT) against Al-Qaeda in Afghanistan and Iraq in an effort to degrade its capabilities and curb international terrorism. And, while there has been a substantial decline in the number of worldwide terrorist attacks since 2007, conclusions on the success of the GWOT have been mixed and global terrorism continues to evolve.[1]

Today, the threat from terrorist groups is geographically diffused, from a diverse array of actors, and it is proving to be both resilient and adaptive to counterterrorism efforts.[2] In addition, the global jihadist movement continues to decentralise swiftly and now covers a broad swath of territory from the Indian Subcontinent, across the Middle East and the Levant, and throughout northern Africa.[3] Terrorist groups today are keeping pace with the advances in internet technology and social media so as to leverage on said platforms to perpetuate their extremist ideology and encourage individuals to act independently in support of their global movement. Consequently, this has led to the rise of 'home-grown', self-radicalised domestic terrorists such as Major Nidal Hasan, who was prosecuted for the 2009 Fort Hood shooting, and the Tsarnaev brothers, perpetrators of the Boston Marathon bombing in April 2013. However, while the use of internet by terrorist groups to spread their ideologies is not new, it is the strategic and highly exploitative use of social media technologies by emerging terrorist groups such as the Islamic State (IS), which has allowed terrorism to fester even more rapidly than before.[4] And, with increasing findings and reports of self-radicalised local citizens leaving for Syria to join the IS's cause, there is fear that these returning fighters will seek to launch terrorist attacks in their own homeland.

However, the maritime security landscape will continue to evolve. As such, similar to dealing with global terrorism, the evolving maritime threat environment will have to be addressed through greater inter-agency cooperation, international collaborations and improved information sharing.

Given that the transnational terrorism's centre of gravity lies outside Singapore, a stove-piped approach to internal security and external defence will no longer work. As such, the SAF has undertaken various approaches, both internationally and domestically, to counter the threat of terrorism. Internationally, the SAF has supported the US efforts in Afghanistan and Iraq, and enhanced inter-military cooperation and collaboration in collective action against terrorism through existing defence co-operation frameworks such as the Association of Southeast Asian Nations (ASEAN) Defence Ministers' Meeting-Plus (ADMM+). Domestically, the SAF has sought to enhance her domestic peace-time counter terrorism capabilities. These include amending the SAF Act in 2007 to give the SAF additional powers against potential terror suspects, the setting-up of the Special Operations Task Force in 2009 equipped with the capabilities and equipment for peacetime contingencies, and the strengthening of interoperability between multiple agencies such as the Singapore Police Force through the Northstar series of exercises.[5]

Moving forward, Singapore continues to recognise the geographically-diffused nature of terrorism and

Cyberpioneer

Special Operations Task Force soldiers conducting an assault on terrorists during a training exercise.

the need for the international community to work closely to counter this threat. As such, the SAF will have to continue leveraging upon its defence co-operation frameworks so as to seek long-term and sustainable solutions to address regional and international terrorism issues. With Singapore currently looking at how it can be a preferred partner in the fight against emerging terrorist organisations such as the Islamic State, future participation by the SAF in coalition-led efforts is also possible.[6] In this regard, the SAF will have to keep pace with developments in counter-terrorism capabilities while ever-strengthening its interoperability with foreign militaries through exercises such as the Joint Counter Terrorism exercise conducted together with the Indonesian National Defence Forces.[7]

To deter the rise of self-radicalised 'home grown' terrorists, the SAF must continue to work closely with inter-governmental agencies in the area of intelligence sharing and in building psychological resilience against terrorism through Singapore's Total Defence framework. To this end, the SAF must continue to actively leverage on the use of social media as a platform to provide counter-narratives against terrorist ideologies and shape Singaporean's confidence in the SAF's capabilities to deal with the evolving terrorist threats.

Global Maritime Security

Singapore is highly dependent on its strategic location along key sea lanes of communication for trade and commerce. As such, Singapore has an interest in preserving freedom of navigation and the safety of international shipping, and in combating threats at sea such as piracy and maritime terrorism. However, due to the trans-boundary nature of these threats and the recognition that no one country or agency is able to tackle the full range of maritime security issues by itself, countries have banded together to secure these sea lanes despite differences in political outlook and national interests.[8]

For Singapore, the SAF has played an active role in supporting the international fight against piracy since 2009 through the deployment of task groups under the ambit of the multinational Combined Task Force 151 in the Gulf of Aden. Regionally, the SAF has contributed to maritime security efforts in the Strait of Malacca through initiatives such as the Malacca Strait Patrols and the setting up of the Republic of Singapore Navy's Information Fusion Centre (IFC).[9]

However, the maritime security landscape will continue to evolve. As such, similar to dealing with global terrorism, the evolving maritime threat environment will have to be addressed through greater inter-agency cooperation, international collaborations and improved information sharing. As the SAF seeks to leverage on the capabilities of IFC in this regard, there is a need for the SAF to address the concerns and risks of information management and sharing. In addition, the SAF would have to create information sharing systems to facilitate interoperability among information-sharing partners. Lastly, the SAF will have to sustain the environment of mutual trust so as to promote integration among information-sharing partners.

Operations Other Than War

Since 1970, the SAF has participated in a number of UN peace support operations and HADR missions at both regional and international levels. This is driven by the belief that the UN is an important institution for upholding international peace and

The 145-strong task group from the SAF patrolling the Gulf of Aden in 2012.

order, and in providing humanitarian assistance to countries in need.[10] With the increased interconnectedness of economies, the effects arising from natural disasters and pandemics can have global consequences. A case in point has been seen in the spread of the Ebola virus—a disease which before 2014 was mostly confined to remote African villages, but has since gone global and is now sparking fear in financial markets.[11] As such, the transnational nature of these global events has drawn the attention of various international organisations, states and their militaries.

The role of the military in OOTW has increased because disasters such as Hurricane Katrina and the Asian Tsunami have highlighted how useful certain military capabilities, such as strategic airlift and sealift, can be when first responders find themselves overwhelmed. In June 2010, the defence ministers of New Zealand, Chile and Malaysia forcefully addressed the Shangri-La Dialogue, calling for disciplined and well-equipped forces that are able to bring relief at short notice.[12] OOTW capabilities, especially in the area of HADR, are therefore increasingly becoming a core task for defence forces.

The SAF recognises the increasing role of the military in OOTW and is investing in the development of full spectrum capabilities as part of its 3rd Generation transformation. However, operational and defence relations challenges in building up such capabilities remain. Firstly, the expeditionary nature of deployment for OOTW demands that the SAF posseses a high-level of operational readiness in both conventional and OOTW capabilities. As such, additional resource investments in manpower, equipment and training have to be made

Cyberpioneer

SAF personnel unloading relief supplies following Typhoon Haiyan in the Philippines in 2013.

due to fundamental differences between the two capabilities. Secondly, OOTW, especially in the area of HADR, continues to be a predominantly civilian function. As such, international norms may place limitations on the use of foreign military assets and thereby limit the extent to which the SAF can project its assistance. Thirdly, a multi-national effort is often required in responding to HADR operations and this poses challenges in the area of interoperability. Lastly, the projection of military forces across national and cultural borders will require the SAF to build up the cultural quotient of our people so that personnel are sensitive to the cultural nuances of the local community as they execute their operations.

To address the first challenge, the SAF needs to consider how it can synergise commonalities between conventional and OOTW capabilities amidst the finite resources that it possesses. These areas of commonality could include equipment, logistics systems and processes, and command and control infrastructure and linkages. At the organisational level, organisation structures can also be tweaked to facilitate seamless transition between conventional and OOTW operations. In addressing the second challenge, the SAF must equip its war-fighters with a clear understanding of its role as the first responders in HADR missions and on how military capabilities for HADR have to be translated in the civilian context so as to eventually allow for the smooth handover of relief operations to civilian agencies. To address the third challenge, the SAF must continue to strengthen its defence relations and cooperation with foreign militaries to enhance interoperability in HADR operations. In this regard, the conduct of the first Humanitarian Assistance and Disaster Relief and Military Medicine exercise in 2013 by the ADMM+ group and the set-up of the Changi Regional HADR Coordination Centre (RHCC) in 2014 were first steps towards achieving this.[13] Finally, in strengthening the cultural quotient of its warfighters, the SAF can continue to leverage on the cultural exposure opportunities provided by its numerous overseas detachments and exercises.

REGIONAL GEOPOLITICAL CHALLENGES

The Asian-Pacific region has seen significant developments in its geopolitical landscape in recent years. China is asserting its influence in the region and has increased its pursuit of territorial claims in the East China and South China seas. Meanwhile, the US under the Obama administration, announced in 2011 that it is shifting its strategic 'pivot' from the Middle East to Asia so as to expand and consolidate its significant role in the Asia-Pacific, particularly in the southern part of the region.[14]

As such, Singapore, moving forward, will need to retain its relevance by seeking to facilitate this re-balancing of US-China presence in the region. Specifically in the area of defence diplomacy, the SAF will need to continue investing in multilateral dialogues and security and diplomatic co-operation to address issues of shared concern between the US, China and ASEAN.

Reactions to these developments by ASEAN members have been mixed, with those involved in territorial disputes with China expressing relief at the renewed engagement of the US, while others warn of the need to avoid tensions with China as the US re-engages the Asia-Pacific. Nonetheless, ASEAN countries have mostly sought to avoid siding openly with the US or China.[15] In the case of Singapore, Singapore's Defence Minister Dr Ng Eng Hen has said that, "the US, as a resident power in the Asia-Pacific for the past 50 years, needs to continue that role as a stabilising force in the region."[16] As such, balancing the roles of Washington and Beijing in the Asia-Pacific region is an important goal of Singapore's foreign policy.[17]

Singapore has enjoyed strong defence relations with the US and has supported the US military's presence in the region through the provision of logistics support. In 2005, Singapore's defence relationship with the US was elevated to a new level with the establishment of a formal strategic military partnership agreement.[18] However, the emergence of China's influence in the region has not gone unnoticed. As such, after several decades of keeping Beijing at arm's length, Singapore has, since 2000, gradually increased security and defence cooperation with China, including high-level dialogues and joint exercises.[19]

Moving forward, the SAF needs to continue to recognise the importance of helping Singaporeans understand the evolving security challenges facing Singapore, the need for the SAF to protect Singapore's strategic interests and the relevance of NS.

While it is uncertain as to how US-China relations in the Asia-Pacific will evolve, Singapore's Prime Minister Lee Hsien Loong believes that there is enough common ground for the US and China to accommodate each other.[20] As such, Singapore, moving forward, will need to retain its relevance by seeking to facilitate this re-balancing of US-China presence in the region. Specifically in the area of defence diplomacy, the

The first batch of the SAF Volunteer Corps reciting the national pledge at the end of their basic training.

SAF will need to continue investing in multilateral dialogues and security and diplomatic co-operation to address issues of shared concern between the US, China and ASEAN. Such diplomatic platforms include groups such as the Five Power Defence Arrangements (FPDA), ASEAN Defence Ministers Meeting-PLUS (ADMM+) and the ASEAN Regional Forum. By leveraging on these platforms, Singapore and the SAF can then deal with the US and China from a position of strength, without which it would be unable to do so.

THE CHALLENGE OF AN INCREASINGLY ARTICULATE POPULATION

Having lived in relative peace and prosperity since their country's independence, Singaporeans have become increasingly expressive about their views towards national defence issues such as defence spending, the role of women in the SAF and the relevance of National Service (NS). This poses a challenge to the SAF as it seeks to engage a generation that is more articulate, technologically adept and IT savvy. To compound the challenge further, all full-time National Servicemen by 2020 would have been born in the 21st century, raised in affluent Singapore, and have no direct memories of the country's early struggles. As such, there is also a need for the SAF to ensure that the defence of Singapore and the institution of NS remain relevant and responsive to the new generation.

The SAF recognises the need to engage Singaporeans on matters of defence and has sought to do so through social media platforms, community engagement programmes and partnership programmes with schools.[21] In addition, the SAF has engaged Singaporeans on issues pertaining to the institution of NS through the Committee to Strengthen National Service (CSNS), which was set up in 2013 and has recently released its findings and recommendations. Various initiatives ranging from better vocational matching and recognition benefits, to the setting up of the SAF Volunteer Corps, were implemented following the CSNS recommendations. However, what is more notable is that these initiatives were a result of the collaborative effort in allowing Singaporeans to shape certain policies of the SAF.

Moving forward, the SAF needs to continue to recognise the importance of helping Singaporeans understand the evolving security challenges facing Singapore, the need for the SAF to protect Singapore's strategic interests and the relevance of NS. In this regard, the SAF will need to continue developing the strategic narratives pertaining to Singapore's defence and effectively communicate it through leveraging upon new advances in social media. Secondly, in ensuring that NS continues to be relevant and responsive to the new generation, the SAF must see through the implementation of all accepted CSNS recommendations. Lastly, to satisfy the needs of an increasingly articulate generation, the SAF must identify ways in which collaborative efforts can be taken to address key concerns that Singaporeans may have on Singapore's national defence.

CONCLUSION

The developments over the past 15 years in the areas of non-traditional transnational security threats, regional geopolitics and an increasingly articulate Singaporean population have provided a glimpse to the challenges the SAF could face in the future. Through the build-up of new capabilities, strengthening of defence co-operation with foreign militaries and stepping-up of its engagement efforts with Singaporeans, the SAF will be able to address these challenges and continue to assure the peace and security of Singapore.

BIBLIOGRAPHY

Abdul-Ahad, Ghaith. "Syria is not a revolution any more – this is civil war." (*The Guardian*, 2013). http://www.theguardian.com/world/2013/nov/18/syria-revolution-civil-war-conflict-rivalry.

Anderson, Nicholas D. ""Re-defining" International Security." The Josef Korbel Journal of Advanced International Studies, 2012.

Andrews, Natalie, and Felicia Schwartz. "Islamic State Pushes Social-Media Battle With West." (*The Wall Street Journal*, 2014). http://online.wsj.com/articles/isis-pushes-social-media-battle-with-west-1408725614.

Anti-Defamation League. *Homegrown Islamic Extremism in 2013: The Perils of Online Recruitment & Self-Radicalization*. 2014. http://www.adl.org/assets/pdf/combating-hate/homegrown-islamic-extremism-in-2013-online-recruitment-and-self-radicalization.pdf.

"Defence Policy & Diplomacy." (*Ministry of Defence*, Singapore, 2012).

http://www.mindef.gov.sg/imindef/key_topics/defence_policy.html.

Freeman, Colin. "Who is in the anti-Islamic State coalition and what they are contributing?" *The Telegraph*. September 26, 2014.

Jane's Defence Weekly. "Briefing: Punching above its weight." February 9, 2012.

Jochems, Maurits. "NATO's Growing Humanitarian Role." (*NATO Review*, 2006). http://www.nato.int/docu/review/2006/issue1/english/art4.html.

Ow, Gary. "Information Sharing: A Singapore Perspective." *The Information Fusion Centre: Challenges and Perspectives, Pointer, Journal of the Singapore Armed Forces Supplement*, 2011.

Song, MAJ Samuel Yong Chiat. "The Global War On *Terror: The Most Extensive and Successful Coalition Ever?" Pointer, Journal of the Singapore Armed Forces*, 2012: v._38 n._2.

Spykerman, Kimberly, and Olivia Siong. "NS Must be Relevant and Responsive to New Generation of Singaporeans: Defence Minister." (*Channel NewsAsia*, 2014). http://lkyspp.nus.edu.sg/ips/wp-content/uploads/sites/2/2014/05/CNA_NS-Must-be-Relevant-and-Responsive-to-New-Generation-of-Singaporeans_220514.pdf.

Tiezzi, Shannon. "How Disaster Relief Can Save China-ASEAN Relations." (*The Diplomat*, 2014). http://thediplomat.com/2014/10/how-disaster-relief-can-save-china-asean-relations/.

Traynor, Ian. "Major terrorist attack is 'inevitable' as Isis fighters return, say EU officials." (*The Guardian*, 2014). http://www.theguardian.com/world/2014/sep/25/major-terrorist-attack-inevitable-isis-eu.

Watkins, Derek. "Territorial Disputes in the Waters Near China." (*The New York Times*, 2014). http://www.nytimes.com/interactive/2014/02/25/world/asia/claims-south-china-sea.html?_r=0.

Yeong, LTC Chee Meng, MAJ Aaron Tan, MAJ Dean Tan, and CPT Jerediah Ong. "RSAF in Operations Other Than War - The Challenges." *Pointer, Journal of the Singapore Armed Forces*, 2007: v. 33 n._1.

ENDNOTES

1. Rogers, Abby. "FBI Reports A Startling Decline In Global Terrorism." (*Business Insider*, 2012). http://www.businessinsider.com/fbi-terrorist-trends-for-2011-2012-10?IR=T&.

2. Rasmussen, Nicholas. "Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland." *Hearing before the Senate Committee on Homeland Security and Governmental Affairs*. September 10, 2014.

3. Ibid.

4. Rivers, Dan. "How terror can breed through social media." (*CNN*, 2013). http://edition.cnn.com/2013/04/27/world/rivers-social-media-terror/.

5. Popatlal, Asha. "SAF given new powers to deal with changed security landscape." (*Channel NewsAsia*, 2007). http://www.channelnewsasia.com/stories/singaporelocalnews/view/277507/1/.html.

   Wong, Lester. "Minister for Defence visits the Special Operations Task Force." (*Ministry of Defence Singapore*, 2011).
   http://www.mindef.gov.sg/imindef/mindef_websites/atozlistings/army/army_news/News_Archive/2011/Sep2011/DM_SOTF.html.

   "Fact Sheet: Exercise Northstar VIII - Testing and Validating the National Maritime Security System." (*Cyber Pioneer*, 2011).
   http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2011/nov/02nov11_news2/02nov11_fs.html.

6. Hussain, Zakir. "Singapore looking at how to be helpful partner in fight against ISIS: PM Lee." (*The Straits Times*, 2014). http://www.straitstimes.com/news/singapore/more-singapore-stories/story/singapore-looking-how-help-counter-isis-pm-lee-20141018#sthash.y37p58n4.dpuf.

Joint Counter-Terrorism Exercise." (*Press Release*, 2012). http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2012/jul/16jul12_nr.html#.VFRu5Ba0SPQ.

8. Lim, LTC Nicholas. "The Information Fusion Centre (IFC) - A Case for Information Sharing to Enforce Security in the Maritime Domain." *The Information Fusion Centre: Challenges and Perspectives, Pointer, Journal of the Singapore Armed Forces Supplement*, 2011.

9. "Fact Sheet: Information Fusion Centre (IFC)." (*Ministry of Defence*, Singapore, 2014). http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2014/apr/04apr14_nr/04apr14_fs.html#.VFSRVxa0SPQ.

10. "Overseas Operations." (*Ministry of Defence*, Singapore, 2014). http://www.mindef.gov.sg/imindef/key_topics/overseas_operations.html.

11. Belluz, Julia. "Ebola has never spread to this many countries before." (*Vox*, 2014). http://www.vox.com/cards/ebola-facts-you-need-to-know/this-ebola-outbreak-started-in-the-rainforest-in-west-africa-and-its.

Hooper, Kristina. "Will the Ebloa Scare Haunt the Stock Market?" (*Allianz Global Investors*, 2014). http://us.allianzgi.com/Commentary/TheUpshot/Pages/will-the-ebola-scare-haunt-the-stock-market.aspx.

12. Fischer, Elisabeth. "Disaster Response: The Role of a Humanitarian Military." (*Army-Technology.com*, 2011). http://www.army-technology.com/features/feature125223/.

13. "SAF and Other Militaries Conclude the ADMM-Plus HADR/MM Exercise." (*Ministry of Defence*, Singapore, 2013). http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2013/jun/20jun13_nr.html#.VFVRfxa0SPQ.

"Fact Sheet: Changi Regional HADR Coordination Centre (RHCC)." (*Ministry of Defence*, Singapore, 2014). http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2014/sep/12sep14_nr2/12sep14_fs.html#.VFVR9_mUeSo.

14. Manyin, Mark E, et al. “Pivot to the Pacific? The Obama Administration's "Rebalancing" Toward Asia.” (*Congressional Research Service*, 2012). http://fas.org/sgp/crs/natsec/R42448.pdf.

15. Comment by Associate Professor Tan See Seng, Deputy Director of the Institute of Defence and Strategic Studies. Quoted from from: Hussain, Zakir. “Special Report; ASEAN Nations Welcome US Pivot”. *Maritime Security Asia*. November 28, 2011. http://maritimesecurity.asia/free-2/asean-2/special-report-asean-nations-welcome-us-pivot/.

16. Ng, Dr Eng Hen. "The Rise of Asia - Reaping Promises, Avoiding Perils" (*Today Online*, 2013). http://www.todayonline.com/commentary/no-title-0.

17. Chanlett-Avery, Emma. "Singapore: Background and US Relations." (*Congressional Research Service*, 2013). http://fas.org/sgp/crs/row/RS20490.pdf.

18. Ibid.

19. Storey, Ian. "China's Bilateral Defense Diplomacy in Southeast Asia." *Asian Security*, v._8 n._3, October 2012: 295-305.

20. Loong, Lee Hsien. "Speech by Prime Minister Lee Hsien Loong at gala dinner hosted by US Chamber of Commerce and US-ASEAN Business Council." (*Prime Minister's Office, Singapore*, 2013). http://www.pmo.gov.sg/content/pmosite/mediacentre/speechesninterviews/primeminister/2013/April/speech_by_prime_ministerleehsienloongatgaladinnerhostedbyuschamb.html#.VFUfKPmUeSo.

21. Gan, COL Siow Huang. "SAF Actively Engages the Community." (*The Straits Times*, 2014). http://www.straitstimes.com/premium/forum-letters/story/saf-actively-engages-the-community-20140130.

ME5 Gabriel Lim Guang Nian is an Air Force Engineer by vocation and is currently serving as the Officer Commanding of Structures Flight in 817 Squadron, Air Power Generation Command. He was awarded the Local Study Award (Engineering) and graduated with 1st Class Honours in Mechanical Engineering from the Nanyang Technological University. ME5 Lim's previous appointments included an overseas posting at the RSAF Peace Carvin II Detachment and a staff appointment at the Air Engineering and Logistics Department.

Information Warfare – The Challenges and Opportunities for Militaries in the Information Age

by CPT Jeffrey Ng Zhaohong

Abstract:

This essay argues that owing to the globalisation of information technology, conflicts today will not only see an increase in the use of information in warfare as an operational and strategic imperative, but also in the use of information as warfare to provide non-kinetic capabilities for achieving strategic outcomes. It then briefly examines the implications for modern militaries and concludes that the information domain will bring game-changing strategic value to militaries that can master both information in warfare and information as warfare.

Keywords: Technology; Information Age; Information Barrage; Availability; Ease of Access

INTRODUCTION

While humans have interacted over long distances for thousands of years, the speed and scale of transnational human interaction around the world has seen an unprecedented surge, enabled by increasingly rapid forms of transportation and communication. This has greatly compressed the time and space needed for the exchange of goods, ideas, knowledge and technology. This increasing interconnectedness, branded as 'globalisation' towards the turn of the millennium, was further amplified by the prolific use of the Internet following the introduction of the World Wide Web.[1] The concomitant revolution in the information technology and communications landscape, touted as the information age, has shaped politics, demolished regimes, given rise to new markets, and offered a bigger voice to the individual. Unsurprisingly, the information age has also heralded transformations in the conduct of present-day military conflicts. This essay argues that owing to the globalisation of information technology, conflicts today will not only see an increase in the use of information in warfare as an operational and strategic imperative, but also in the use of information as warfare to provide non-kinetic capabilities for achieving strategic outcomes. It then briefly examines the implications for modern militaries and concludes that the information domain will bring game-changing strategic value to militaries that can master both information in warfare and information as warfare.

NEW NORMS IN THE INFORMATION AGE

The globalisation of information technology has enabled individuals and organisations to interact at an unprecedented scale and speed. For example, access to the Internet has grown from just 5% in 2000 to over 42% in 2014.[2] With an increasing ease of instantaneous information access, traditional state-driven censorship and media control as a means to regulate and shape public opinions are fast becoming obsolete and counter-productive because individuals have become empowered to scrutinise and challenge

Celebrations in Egypt's Tahrir Square after Vice President Omar Suleiman's statement concerning President Hosni Mubarak's resignation.

the actions of well-established social and government institutions. In parallel, the proliferation of mobile communications, and the rising participation rate in social media over the past decade have enabled individuals to share and shape public opinions, garner support from like-minded individuals, and rapidly self-mobilise for a common cause against governments, as witnessed in the Arab Spring and the various Occupy Movements in 2011.[3] Taken together, societies in the information age possess heightened awareness of the diverse opinions and portrayals of world events, and are less likely to rely solely on the government's interpretation of events. To deal with the increased public demand for accountability and transparency, governments are now compelled to actively engage and convince the public of its legitimacy in order to engender continued support for its actions and policies.

The use of information in warfare to achieve operational objectives has always been an integral arm of military warfare, be it in the forms of covert intelligence or overt domestic propaganda.

The information age has not only altered the social compact within individual states; it has also interwoven states, corporations, and organisations into interdependent networks due to the growing reliance on the use of computers and information systems. In the civilian and commercial domains, the explosive growth of information technology, especially in terms of online storage and network traffic capacity, has accelerated the adoption of electronic systems, as well as vastly increased the dependency on wireless communications to digitise and automate daily tasks. Modern militaries have also leveraged on the available technology to transform their operations using networked concepts.[4] Such network-centric warfare heavily hinges upon a robust and resilient network infrastructure to link together various sensors and shooters with computer systems to vastly speed up the kill cycle. The widespread reliance on networked information systems in state and non-state organisations has also increased the inter-dependency between these entities for functional integrity. Such national-level vulnerabilities, arising from the growing dependence on networked systems, present militaries with both challenges and opportunities in the present-day conflicts.

INFORMATION IN WARFARE - AN OPERATIONAL AND STRATEGIC IMPERATIVE

The use of information in warfare to achieve operational objectives has always been an integral arm of military warfare, be it in the forms of covert intelligence or overt domestic propaganda. However, with the increase in speed and reach of information, any newsworthy conflict will be immediately thrust into the consciousness of the international community, and subjected to scrutiny, debates, and opinions which will shape the portrayal of the parties involved in the conflict. Moreover, traditionally weaker adversaries can leverage on cheap and readily available information technology such as social media platforms and video hosting websites, to wield disproportionate influence over domestic and international masses to systematically undermine the legitimacy and morality of the military and also mobilise local populations to rise up against the invading military. Hence, carefully crafted multi-faceted information operations, as an essential element of an overall military strategy, will become an increasingly pivotal operational and strategic imperative for winning the battle of perceptions, securing operational battle-space, and achieving strategic victory in present-day conflicts.

The centrality of information operations to the strategic success of present-day conflicts is exemplified by contrasting the outcomes of the 2006 Second Lebanon War and the 2009 Operation Cast Lead. Despite the Israeli Defense Force (IDF)'s tactical successes in the Second Lebanon War, Israel was unable to achieve strategic victory against the Hezbollah. In fact, the organisation's charismatic leader, Hassan Nasrallah, was able to emerge from the conflict with his reputation intact.[5] Post-mortem analysis of the conflict indicated that the strategic failure was largely attributed to Israel's inability to paint a coherent narrative to blunt Hezbollah's portrayal of the IDF's disproportionate use of force against civilian victims.[6] For example, the destruction wrought by the IDF's use of air power against civilian buildings provided copious material for Hezbollah's civilian-victim narrative. On the other hand, Hezbollah was able to coerce and manage the international press in Lebanon to ensure the non-existence of Hezbollah's combat imagery, further reinforcing the perception that defenceless Lebanese civilians were being bullied by the IDF.[7] The theme of ‘disproportionality’ resonated with the international audience, and mounted political pressures on Israel, ultimately forcing the IDF to halt its operation before it could achieve its operational objectives.[8]

Learning the strategic significance of a coherent information effort, Israel established the Directorate of National Information in 2007 to coordinate and develop inter-ministerial plans and strategies for a whole-of-government approach in information operations during national emergencies.[9] The increased emphasis on the information battle was evident in Operation Cast Lead in 2009, during which the Israeli government was able to consistently portray an overarching narrative against the Hamas through a coordinated inter-ministerial approach.[10]

Wikipedia

Smoke rising from a bombed building in Lebanon during the Second Lebanon War.

This was further complemented by the innovative use of social media sites to disseminate imagery from the soldiers' cameras to the international audience in a timely manner. The real life ground and Unmanned Aerial Vehicle (UAV) footages enhanced the IDF's emotive connection with the audience and authenticated claims of its relentless efforts in minimising collateral damage and civilian casualties. Consequently, Israel was able to secure the operational battle-space necessary for the IDF to achieve its operational objectives without overwhelming political incrimination.

The strategic failure of the Second Lebanon War and the relative success in Operation Cast Lead illustrated that in the information age, a coherent and proactive information campaign waged on traditional and online media must complement traditional operations in order to dominate the international mindshare with favourable portrayals and secure strategic political legitimacy. Winning the battle of perceptions is not only important for freedom of operations, but also pivotal to the strategic outcome of the conflict.

INFORMATION AS WARFARE – CYBER WARFARE

Beyond the use of information to shape strategic narratives, the proliferation and near-universal accessibility of information technology can potentially supplant the Clausewitzian industrial-era model of destruction-driven warfare with an information age model of disruption-based operations waged through the use of smart technologies in the cyberspace.[11] The exploitation of national-level vulnerabilities in information networks opens up possibilities for non-lethal cyber attacks to disrupt, incapacitate, defeat or deter an adversary, thereby attaining strategic objectives without resorting to resource-intensive conventional kinetic operations. As both society and militaries become more networked and reliant on computers and information systems, the cyber domain will likely become the predominant battle-space for conflicts in the information age because of the strategic strengths conferred by cyber warfare.

As both society and militaries become more networked and reliant on computers and information systems, the cyber domain will likely become the predominant battle-space for conflicts in the information age because of the strategic strengths conferred by cyber warfare.

Firstly, the rapid growth in worldwide interconnectedness of online systems allows operations in cyberspace to provide global reach, even to areas where access is denied to other domains. This is unlike traditional military operations, which are often confined by geographic limitations. Compared to the projection of troops into contested areas, cyber operations can also provide access without physical risks to the operators. Another alluring advantage of cyber operations is its ability to strike with speed and precision. Computer virus dissemination through online networks can occur literally at the speed of light through fibre optic cables, and can be selective in targeting specific networks to achieve intended effects with minimal collateral damage. These strengths were well demonstrated in the employment of the malware 'Stuxnet' to disrupt the Iranian nuclear centrifuges by targeting the industrial control systems.[12] The malware attack, allegedly a joint US-Israel endeavour, damaged over a thousand centrifuges at the Natanz uranium enrichment facility, and successfully delayed Iran's acquisition of a nuclear device without any forward deployment of troops, breach of Iranian airspace, loss of life, or physical damage to the nuclear facility.[13] The 'Stuxnet' attack also demonstrated another strategic advantage of warfare in the cyber domain – anonymity. The high degree of decentralisation and peer-to-peer networks characterising the cyber domain makes it challenging to trace the evidentiary trail to originators of the cyber attacks.[14] This confers great latitudes of action with limited attribution and hence, minimises potential social and political backlash on the perpetrators.

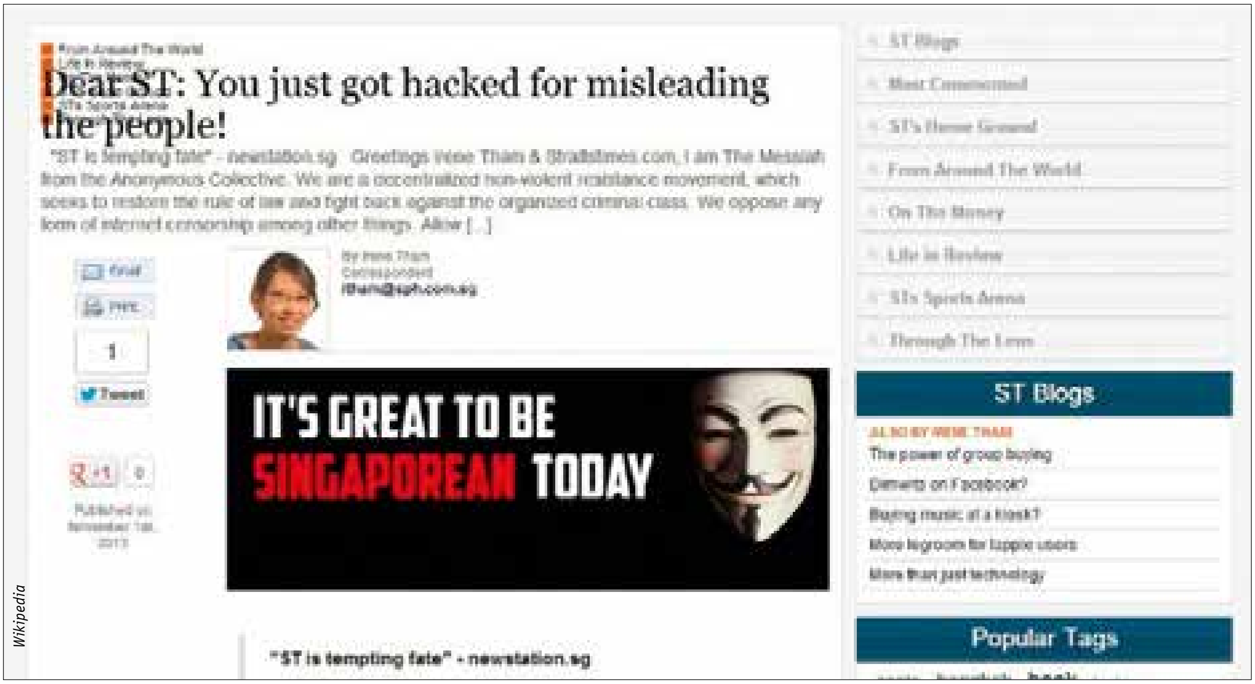
The strengths offered by cyberspace favours offensive operations over defence. Moreover, unlike traditional weapons, the tools needed to wage cyber warfare may be freely accessible on the Internet or traded in underground markets.[15] This creates greater asymmetry in a conflict by allowing state and non-state actors that have limited resources and are weaker in traditional domains of warfare to exploit the cyber domain for strategic effects of disruption, and even destruction of system capabilities. For example, in 2013, a small group of hackers named 'the Anonymous Collective' or 'the Messiah' allegedly managed to disrupt the normal functioning of 19 Singapore governmental websites.[16] Paradoxically, the more sophisticated the fighting force, the higher the likelihood of suffering from cyber attacks. The consequences of a successful attack are also greater due to the systemic dependency of routine operations on the integrity of networks and computer systems. In light of the strategic threats and opportunities offered by the use of the information domain, leading militaries such as the United States (US) Air Force have stepped up on their efforts in building up cyber warfare capabilities.[17] Singapore has also recognised the importance of a co-ordinated national approach against cyber threats to its national infrastructure, and in response, has established the Cyber Security Agency to strengthen cyber security in sectors critical to the nation's survivability.[18]

IMPLICATIONS FOR MODERN MILITARIES

With the growing strategic importance of the information domain for present-day conflicts, modern militaries will be increasingly compelled to focus on information operations and cyber warfare capabilities in order to maintain their strategic edge over other state and non-state actors. To truly harness the strategic value of information operations, modern militaries would need to restructure themselves to be centralised and dedicate focus on planning and orchestrating a coherent strategic narrative. Military operations should also be planned and coordinated to support the strategic campaign message. This is because in today's conflicts, conducting military operations in isolation of a central narrative will run the risk of adversaries using these operations to reinforce their own narratives. In contrast, a unified message stemming from complementary operational effects would serve to solidify the military's legitimacy, and allow the military to quickly translate operational success into strategic victories. For example, during Operation Cast Lead, in a bid to maintain its moral standing and to erode the Hamas' civilian-victim narrative, the IDF deliberately deployed Combat Camera teams to provide footages demonstrating the Hamas using mosques as weapon caches, and also flew dedicated sorties to drop leaflets asking civilians to vacate the area before each air strike.[19]

Paradoxically, the more sophisticated the fighting force, the higher the likelihood of suffering from cyber attacks.

Similarly, the strategic importance of cyber operations would compel modern militaries to develop



From Around The World
Life In Review
STs Sports Arena

Dear ST: You just got hacked for misleading the people!

"ST is tempting fate" - newstation.sg Greetings Irene Tham & Straitstimes.com, I am The Messiah from the Anonymous Collective. We are a decentralized non-violent resistance movement, which seeks to restore the rule of law and fight back against the organized criminal class. We oppose any form of internet censorship among other things. Allow [...]

By Irene Tham
Correspondent
itham@sph.com.sg

Published on November 1st, 2013

"ST is tempting fate" - newstation.sg

Wikipedia

A screenshot of a Singapore website that was being hacked into by the group known as 'Anonymous'.

cyber warfare capabilities in a coherent approach as a strategic capability, instead of ad-hoc enhancements to existing capabilities. Militaries pursuing cyber operations as an individual military domain should also aim to fulfil the full range of military objectives, including physical destruction in order to harness the strategic gains of cyber warfare. Advanced militaries facing manpower and budgetary constraints would likely spearhead the development and employment of cyber attack capabilities given the high resource efficiency of cyber operations. Consequently, robust cyber defence capabilities would become staple operational requirements for undisrupted military operations in the present day. Given the convergence between defence against military cyber attacks and commercial cyber crime, militaries could explore synergistic inter-ministerial developments, leverage creatively on commercially available technology, and adopt established commercial cyber defence protocols in order to quickly develop sustainable cyber defence capabilities.

CONCLUSION

Globalisation of information access has exponentially increased the interconnectedness of human consciousness and computer systems through worldwide proliferation of networked information technology. Consequently, present-day conflicts are waged under the scrutiny of the international audience. Hence, information operations in warfare will play an increasingly pivotal role as an operational and strategic imperative to cultivate favourable political atmospherics for continued freedom of action. The growing dependence on the cyber space in the information age offers cyber warfare as an alternative realm for waging present-day conflicts. The widespread accessibility of information technology provides state and non-state actors with the necessary tools for both information operations and cyber attacks, tilting the balance against traditionally superior fighting forces. To ensure strategic success in the information age, militaries and their governments must rapidly re-examine their organising principles and adopt current technologies to develop comprehensive information warfare capabilities in line with a coherent national strategy.

BIBLIOGRAPHY

Albright, David, and Andrea Stricker. “Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target?” Institute for Science and International Security, November 17, 2010.

http://isis-online.org/isis-reports/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-is-irans-ce/8.

Allagui, Ilhem, and Johanne Kuebler. “The Arab Spring and the Role of ICTs.” International Journal of Communication 5 (2011): 1435-1442.

Bishop, Matt, and Emily Goldman. “The Strategy and Tactics of Information Warfare.” Contemporary Security Policy 24 (2003): 113-139.

Catignani, Sergio. “Variation on a Theme: Israel's Operation Cast Lead and the Gaza Strip Missile Conundrum, ” The Rusi Journal, 154 (2009): 66-73.

Cebrowski, Arthur K, and John H. Garstka. “Network-Centric Warfare: Its Origin and Future.” US Naval Institute Proceedings Magazine 124 (1998), 28-35.

Greenberg, Andy. “Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits.” Forbes, March 23, 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-forzero-days-an-price-list-for-hackers-secret-software-exploits.

International Monetary Fund. "Issues Brief - Globalization: A Brief Overview." Accessed February 1, 2015. http://www.imf.org/external/np/exr/ib/2008/053008.htm.

Internet World Stats. "World Internet Users Statistics and 2014 Population Stats." Accessed February 1, 2015. http://www.internetworldstats.com/stats.htm.

Kalb, Marvin, and Carol Saivetz. “The Israeli—Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict.” The International Journal of Press/Politics 12 (2007): 43-66.

Lee, Terence. “19 Singapore Government Websites Taken Down Simultaneously for “Planned Maintenance”.” Tech in Asia, November 2, 2013.

https://www.techinasia.com/16-singapore-government-websites-simultaneously-planned-maintenance.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22 (2013): 365-404.

Nakashima, Ellen. "Pentagon to Fast-Track Cyberweapon Development." The Washington Post, March 18, 2012.

http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

Snyder, Michael D. “Information Strategies Against a Hybrid Threat: What the Recent Experience of Israel Versus Hezbollah/Hamas Tell The US Army.” In Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD, edited by Scott C. Farquhar, 103-146. Fort Leavenworth, Kansas: Combat Studies Institute Press, 2009.

Stewart, Frances. "Global Economic Influences and Policies towards Violent Self-Determination Movements: An Overview.” In Globalization, Violent Conflict and Self-Determination, edited by Valpy FitzGerald, Frances Stewart and Rajesh Venugopal, 20-47. New York: Palgrave Macmillan, 2006.

Tham, Irene. “New Cyber Security Agency to be set up in April, Yaacob Ibrahim to be Minister in Charge of Cyber Security.” The Straits Times, January 18, 2015. http://www.straitstimes.com/news/singapore/more-singapore-stories/story/national-cyber-security-efforts-fall-under-new-cyber-sec.

The Statistics Portal. "Number of Global Social Network Users 2010-2018.” Accessed February 5, 2015.
http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

Wilson, Clay. “Cyber Crime.” In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, 415-436. Washington, DC: National Defense University Press, 2009.

ENDNOTES

1. IMF Staff, Globalization: A Brief Overview, (International Monetary Fund, 2008)
http://www.imf.org/external/np/exr/ib/2008/053008.htm.

2. "World Internet Users Statistics and 2014 Population Stats," Internet World Stats, accessed February 1, 2015, http://www.internetworldstats.com/stats.htm.

3. Ibid.

4. Number of Global Social Network Users 2010-2019 (in billions), (statista, The Statistics Portal)
http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

Stewart, Frances, Global Economic Influences and Policies towards Violent Self-Determination Movements: An Overview, (New York: Palgrave Macmillan, 2006).

Allagui, Ilhem and Kuebler, Johanne, The Arab Spring and the Role of ICTs, (International Journal of Communication 5, 2011)

6. Arthur K. Cebrowski and John H. Garstka, Network-Centric Warfare: Its Origin and Future, (*US Naval Institute Proceedings Magazine*, 1998), v._124

7. Michael D. Snyder, Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD, (*DIANE Publishing*, 2010), 115.

8. Ibid., 120.

9. Kalb, Marvin and Saivetz, Carol, THE ISRAELI-HEZBOLLAH WAR OF 2006: The Media As A Weapon In Asymmetrical Conflict, (Harvard University, 2007), 43-66.

10. Ibid., 55.

11. Snyder, Information Strategies, 126.

12. Ibid.

13. Bishop, Matt and Goldman, Emily, The Strategy and Tactics of Information Warfare, (*Contemporary Security Policy* 24, 2003), 113.

14. Albright, David and Andrea Stricker, Andrea, Stuxnet Worm Targets Automated Systems for Frequency Converters: *Are Iranian Centrifuges the Target?, Institute for Science and International Security*, 2010) http://isis-online.org/isis-reports/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-is-irans-ce/8.

15. Jon R. Lindsay, Stuxnet and the Limits of Cyber Warfare, (*Security Studies* 22, 2013)

16. Wilson, Clay, Cyber Crime, Cyberpower and National Security, (*Washington*, DC: NDU Press, 2009)

17. Greenberg, Andy, Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits, (Forbes, 2012) http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-forzero-days-an-price-list-for-hackers-secret-software-exploits.

18. Lee, Terence, 19 Singapore Government Websites Taken Down Simultaneously for "Planned Maintenance", (*Tech in Asia*, 2013) https://www.techinasia.com/16-singapore-government-websites-simultaneously-planned-maintenance.

17. Nakashima, Ellen, Pentagon to Fast-Track Cyberweapon Development, (*The Washington Post*, 2012) http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

18. Tham, Irene, New Cyber Security Agency to be set up in April, Yaacob Ibrahim to be Minister in Charge of Cyber Security, (*The Straits Times*, 2015) http://www.straitstimes.com/news/singapore/more-singapore-stories/story/national-cyber-security-efforts-fall-under-new-cyber-sec.

19. Catignani, Sergio, Variation on a Theme: Israel's Operation Cast Lead and the Gaza Strip Missile Conundrum, (*The Rusi Journal* 154, 2009), 71.

CPT Jeffrey Ng Zhaohong is currently serving as an Officer Commanding in 119 SQN, UAV Command. He is a UAV Pilot by vocation and is a Command Pilot of the Heron 1 UAV. A recipient of the SAF Merit Scholarship in 2008, he graduated from University College London with a Bachelors of Science Psychology with Honours in 2011, and subsequently from the University of Edinburgh with a Masters of Science in Performance Psychology.

Espousing the Utility of Contemporary Air Power in the Strategic Domain for Small States

by LTC Victor Chen Kanghao

Abstract:

In this essay, the author examines how air power, defined as the ability to project military power or influence through the medium of the air to achieve strategic, operational or tactical objectives, may be utilised by the armed forces of small states like Singapore in the modern context. Firstly, using the example of Israel, he challenges critics of the early proponents of strategic bombing such as Douhet, arguing that traditional bombardment still has a decisive effect on the outcome of war if used effectively and with precision. He then explores other strategic applications of air power for small states, namely in intelligence-gathering, psychological operations and logistics. Lastly, apart from displaying 'hard power', he contends that a strong air force may help small states accumulate 'soft power' through developing close relationships with other armed forces and engaging the international community through Humanitarian Assistance and Disaster Relief (HADR) operations.

Keywords: Air Power; Strategic Bombardment; Small States; Psychological Operations; Hard and Soft Power

INTRODUCTION

Air Power is the ability to project military power or influence through the medium of the air to achieve strategic, operational or tactical objectives.[1] At the turn of the 20th century, early proponents of air power, such as Giulo Douhet, William Mitchell and de Seversky, contend that the command of the air is a necessary element to determine the victors of war.[2] These luminaries focused primarily on advocating strategic bombardment as the means to extract the full utility of air power, asserting that devastating attacks from the air would lead to decisive victories without the need to first defeat the enemy's ground forces. Since then, experience gleaned from contemporary wars and conflicts in Vietnam, Kosovo and Gaza has shed light on some of the fallacies of these assertions.[3] Furthermore, the evolving strategic and operational security landscape, coupled with technological advances in aircraft performance and weaponry, has necessitated the development of new applications of air power, beyond the traditional strategic bombardment role.[4] This has effectively thrust air power from the periphery into the forefront as a valuable trump card in the geopolitical bargaining table. Aptly encapsulating the essence and strategic nature of air power, General Omar Bradley sursmises: "Air power has become predominant... both as a deterrent to war, and in the eventuality of war, as the devastating force to destroy an enemy's potential and fatally undermining his will to wage war."[5]

For small states such as Israel, New Zealand and Singapore, constraints in resources and geography have hampered their abilities to build sizeable armed forces to meet the challenges of their respective geostrategic environments. Greater efforts would thus need to be taken to circumvent these limitations, through meticulous force planning and judicious investment in military capabilities, prolific use of the latest advanced technologies, as well as innovative force employment.[6] Recognising the ability of air power to rapidly respond to national defence or mount lethal offensives with inherent speed, range, and flexibility, Singapore has built up a strong air force as the backbone of its military.[7] With a credible air force, a strong deterrence is ensured, and should hostilities ensue, the full range of retaliatory options will be available to ensure a swift and decisive victory.[8]

This essay will confine the discussion to the strategic-level, with a more long-term view in terms of time horizon compared to the operational and tactical domains.[9] Mission objectives at the strategic-level typically involve the progressive destruction and disintegration of the enemy's war-fighting capacity and will to wage war, stretching over the entire campaign.

Upon reviewing the arguments on air power's traditional function of strategic bombardment in today's context, the case for its applicability by small states will be discussed. The position elucidated is that the utility of air power still stands for small states, and that strategic bombardment is still a viable option, provided it is adapted to suit the context of small armed forces. The essay will go on to discuss the other strategic applications of air power, and how the applications are relevant to small armed forces such as the Singapore Armed Forces (SAF).

RELEVANCE OF STRATEGIC BOMBARDMENT AS A CONTEMPORARY AIR FORCE MISSION SET

Critics of air power hail that the conclusions reached in the propositions of Douhet and his contemporaries on strategic bombardment were based on unrealistic assumptions and overly optimistic

Wikipedia

Collateral damage in Gaza city due to bombing during the Israeli-Palestinian conflict.

extrapolations of available data.[10] Lessons gleaned from the Vietnam and Kosovo wars in general show that sheer numbers and scale of bombing alone were insufficient to overcome the enemy.[11] In the air war over Gaza, Hamas used the Palestinian civilian population as shields, by placing weapons caches and rocket launcher positions right next to schools, mosques and hospitals.[12] This made them difficult to target, and if the decision to strike is made, risk of high civilian casualties and collateral damage will be brought to bear. In the recent months leading up to the winter of 2014, as the United States (US) scaled up the bombing campaign against Islamic State (IS) militants in Syria and Iraq, it became increasingly clear that the airstrikes were proving insufficient in 'destroying' or even 'degrading' IS forces. Analysts have attributed this largely to the non-traditional structure of the IS, where many of the IS targets are non-static and temporary, coupled with the fact that IS forces were adept at blending into the civilian population.[13] These examples are stark reminders that the enemy does not always adhere to convention, and that traditional notions of strategic bombing will prove ineffective against such an enemy.

However, in Douhet's defence, his theories were formulated at a time before the invention of radar or effective forms of air defence. Outdated as they are in today's context, given technological advances and changes to the strategic landscape, relevant lessons can still be drawn from Douhet's tenets of strategic bombing. Winn expounds that Douhet's key axioms can be summarised as follows: first, in order to assure victory, it is necessary to conquer and command the air; second, the advantage of speed and elevation in the three-dimensional arena of air warfare have made it impossible to take defensive measures against an offensive air strategy; third, airpower should be used against the enemy's 'vital centre'—the enemy's centres of population, government and industry.[14] Winn goes on to explain that when translated to the contemporary context, the axioms can be directly mapped to convey: (1) gaining air superiority; (2) suppression of enemy air defences; and (3) attacking the enemy's centre of gravity. Indeed, these are doctrinally-relevant concepts in modern war-fighting, with the Pacific theatre in World War II (WWII), Operation Linebacker in the Vietnam War and Operation Desert Storm as examples of strategic bombing being used to great effect. Adding to the case for the relevance of strategic bombing, Edward Warner and Robert Futrell separately concluded that Douhet's validity has become stronger with time, and that the arrival of the nuclear and thermonuclear age further strengthened the theory's applicability in modern day conflicts.[15]

The overarching strategic objective is to disrupt and dislocate the enemy's overall warfighting capabilities, while using the least amount of resources in order to conclude hostilities in the shortest possible time. This will allow the attainment of a quick and decisive victory while avoiding the undue strains of fighting a protracted war.

While it is apparent that it is not possible to break an adversary's will to fight through bombing alone, it has been generally agreed that air power will have a decisive influence on the outcome of war.[16] However, for air power to be relevant in the modern battlefield, the application of strategic bombardment needs to exhibit more 'finesse', as opposed to the mass attack doctrine elucidated by Douhet. This statement particularly holds true for small air forces such as Israel and Singapore.

Wikipedia

Smoke rising from a bombed building in Lebanon during the Second Lebanon War.

MEANS BY WHICH SMALL ARMED FORCES CAN EFFECTIVELY PROSECUTE STRATEGIC BOMBING

Sanu Kainikara, in discussing small air forces, suggested that the changing nature of war necessitates the development of innovative concepts for military forces to be effective.[17] Only by the effective employment of air power can its potential be truly maximised. To illustrate, at the commencement of the First Intifada in the Israel-Palestinian conflict in 1987, despite the ratio of Israeli to Arab combat aircraft being about one to four, Israel still had the upper hand because of its higher maintenance standards, higher pilot-aircraft ratio and advanced precision weapons delivery systems.

In the case of small states with limited aircraft Order of Battle (ORBAT) size, material and human resources, adhering to the notion of prolonged large scale mass bombing will result in unnecessary depletion of their limited munitions stockpile and in the long run, affect the national economic functions. Take for example a conscript armed force, such as Singapore or Israel. With the state's economy greatly dependent on international trade, tertiary industries and services, should hostilities persist protractedly, economic activity will effectively grind to a slow halt as long as the conscripts are mobilised for war. Thus the selection of targets and weapon-matching needs to be more deliberate, in order to solicit the highest possible strategic effects by striking the enemy’s critical centres of gravity. The overarching strategic objective is to disrupt and dislocate the enemy's overall warfighting capabilities, while using the least amount of resources in order to conclude hostilities in the shortest possible time. This will allow the attainment of a quick and decisive victory while avoiding the undue strains of fighting a protracted war. During the Six-Day War in June 1967, the Israeli Air Force (IAF) dealt a devastating blow to Egypt by launching a massive air raid against Egypt, attacking key military installations, airfields and destroying most of the Egyptian Air Force while the aircraft were still on the ground.[18] Following this successful application of strategic strikes, the Israelis emerged the clear victors, and hostilities were able to cease within six days, with Egypt and its Arab neighbours sullenly accepting a United Nations (UN)-imposed ceasefire.

The advent of Precision Guided Munitions (PGMs) and the concept of Network-Centric Warfare (NCW) are two key resource-saving enablers that small states can rely on to better 'finesse' the conduct of strategic bombing. The paradigm shift that negated the requirement of mass attack from the air can be partly attributed to the rise of PGMs. In Operation Desert Storm, 90% of the targets destroyed were attributed to the effective employment of PGMs, which constituted a mere 8% of the total number of bombs dropped.[19] Thus, mission planning for strategic bombing can now be done in terms of "targets per sortie, instead of sorties per target."[20] Separately, the edge that NCW gives is gained when agents across the spectrum of operations are effectively linked and are able to leverage on superior information to attain a common overview of the battlespace. All available strike assets, be it air-launched or surface-launched, can be optimised and integrated, making the prosecution of the strategic strikes a more deliberate and efficient process. Hence, it is important that small armed forces such as the SAF continue along this development trajectory, in order for strategic bombing to still be relevant in today's context.

Wikipedia

US Air Force aircraft flying over Kuwaiti oil fires during Operation Desert Storm.

The utility of air power does not end at strategic bombing. The next part of the essay will discuss the other strategic applications of air power for small air forces that are outside the domain of strategic bombardment.

NEED FOR STRATEGIC INTELLIGENCE DUE TO THE LACK OF STRATEGIC DEPTH

Unlike large states, small states lack the strategic depth to provide a buffer needed against enemy attacks.[22] Backyard threats from Rockets, Artillery and Mortar (RAM) originating from enemy-controlled territory will be within reach of the small states' city centres and key installations. This, in essence, is an inherent vulnerability, characteristic of small states. To prevent the situation of fundamental surprise, small states need advance warning capabilities of massing enemy forces preparing to mount an offensive, in order to have lead time to prepare itself for the appropriate response. Air power in this instance is particularly effective in conducting strategic Air Intelligence, Surveillance and Reconnaissance (ISR) operations, providing Early Warning Indicators.[23] During the Cuban Missile Crisis, U-2 reconnaissance planes were able to collect imagery evidence to prove that the Soviets have been secretly building nuclear missile silos at America's backyard, in Cuba. This gave the Kennedy Administration sufficient time to draft out the various options to respond appropriately.[24] This underscores the importance of air power to provide the strategic intelligence mission, especially for small states, where the backyard threat is a constant concern.

PARTICIPATION OPERATIONS, PSYCHOLOGICAL OPERATIONS AND STRATEGIC AIRLIFT – INFLUENCING THE OVERALL STRATEGIC CAMPAIGN

As a conflict escalates into a full-blown war, air power can project ground and naval forces expeditiously, which, without an air force, would be “difficult for a small state with limited breakout points.”[25] For instance, during the 1982 Lebanon War, the IAF's operations ensured that the Israeli Army was able to advance rapidly to their objectives, reaching Beirut in merely 3 days.[26] The IAF was tasked to first gain air superiority over Israel and the battlefield. Not only would air superiority protect the state’s civilian populace and industrial assets from an air attack, it also enabled the army to mobilise and deploy its large reserve forces quickly, which have always formed the bulk of its combat formations. The IAF then supported the army’s ground forces by flying battlefield air interdiction and close air support missions, as well as additional duties, such as long-range strike missions against sensitive military and industrial targets in the enemy’s hinterland. Similarly, in the case of Singapore, strong air power will allow the quick attainment of air superiority, after which the air force will have freedom of operations to influence the land and maritime battles.

If conducted appropriately in tandem with kinetic operations, psychological warfare can sway opinions of the populace towards friendly forces and create negative sentiment towards the adversary, with the overall effect of eroding the enemy's will to fight.

Additionally, air power can be used to contribute to Psychological Operations (PsyOps), which involves the planned use of propaganda and other psychological actions to influence the opinions, emotions, attitudes and behaviour of the adversary's military and civilian population. Aircraft will drop leaflets to both inform the local civilians about operations and to shape the battlefield. For example, PsyOps units in Somalia

A UH-60 Black Hawk from the US Army's 350th Tactical Psychological Operations Company dropping leaflets in Iraq in 2008.

conducted over 7 million leaflet drops to explain both why the UN was in Somalia and the details of specific operations.[27] If conducted appropriately in tandem with kinetic operations, psychological warfare can sway opinions of the populace towards friendly forces and create negative sentiment towards the adversary, with the overall effect of eroding the enemy's will to fight.

Lastly, should the task of securing the Lines of Communication (LOC) over sea or land be overly dangerous or time-consuming, strategic airlift will be the only way to deliver supplies, personnel and equipment to the area of operations. This is particularly true for small states, as the lack of strategic depth makes LOC security a more difficult task. Air power can therefore provide the efficient mobility to expedite and facilitate the conduct of operations to enable quicker cessation of hostilities.

AIR POWER AS A LEVER FOR FOREIGN POLICY – DISPLAYING BOTH HARD AND SOFT POWER

The presence of a credible military acts as a form of deterrence, with the overarching objective of compelling the opponent to conform to our intended political will.[28] Air power, with its responsiveness and flexibility in employment, is able to level the playing field for small states in the international arena, through displaying the requisite 'hard power' to provide avenues for enlarging the small state's policy space.[29] In essence, with a credible air force, a small state will be able to project a credible 'threat' of force, to coerce a larger adversary to change its behaviour or to de-escalate tensions.

Additionally, a small state's air force can be used to enhance 'soft power', contributing to the state's peace and security by actively engaging international partners in relationships that will be mutually beneficial.[30] To illustrate, close relationships between Israel's armed forces and military industrial complex with those of the US are beneficial to both states. In the event of a conflict involving Israel and her neighbours, Israel will be able to bank upon these relationships for US assistance, if required.

Lastly, air power can also be used in Humanitarian Assistance and Disaster Relief (HADR) operations, thereby allowing a country to enhance its international standing. In recent years, Singapore has extended HADR to Indonesia, Thailand and the US, thereby increasing diplomatic mileage and accumulating the stock of soft power.[31] Through these operations, the Republic of Singapore Air Force (RSAF) has demonstrated our capability and operational readiness to rapidly respond and project air power where required. Thus, there is also a hard power aspect that further contributes towards the deterrence factor.

In essence, with a credible air force, a small state will be able to project a credible 'threat' of force, to coerce a larger adversary to change its behaviour or to de-escalate tensions.

CONCLUSION

Small states such as Singapore face unique challenges and obstacles in ensuring sovereignty and survival. The solutions to surmount these impediments are often complex to derive and arduous to execute. This essay has provided a mere snapshot of how air power should be judiciously applied by the SAF in our current strategic context and geopolitical climate.

An aircrew from the RSAF prepares to drop a marine marker during the MH370 search operation in 2014.

With the new emerging threats and uncertainties of the future battlespace, the SAF will need to constantly adapt our force structure and paradigms of air power application in order to ensure that our ability to maintain peace, and a rapid return to normalcy, should hostilities ensue, are not compromised.

BIBLIOGRAPHY

Chaim Herzog, *The Arab-Israeli Wars: War and Peace in the Middle East*, Second Vintage Books Edition, July 2005.

CPT Chen, Victor, "Rationalising the Paradigm Shift from Network-Centricity to Knowledge-Centricity," *Pointer*, v. _36, n. _1, 2010.

Dayan, Uzi, "Air Power – The Israeli Perspective," *Military Technology*, v._23, n. _5, May 1999.

De Seversky, Alexander P., *Victory Through Air Power*, New York: Simon & Schuster, 1942.

Douhet, Giulo, *The Command of the Air*, trans Dino Ferrari, Washington, D.C.: Office of Air Force History, 1983.

"Douhet: Still Relevant Today," (*USAF CSC*, 1991), http://www.globalsecurity.org/military/library/report/1991/WGC.htm.

Futrell, Robert, F., Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force: 1907-1960, v._1, Maxwell AFB: Air University Press, 1989.

Garden, Timothy, "Air Power: Theory and Practice," *Strategy in Contemporary World*, ed. Baylis, J.; Wirtz, J.; Cohen, E.; Gray, C.S., Oxford University Press, Chapter 6, 2002.

"Gaza Campaign Highlights Strength, Limitations of Air Power," (*Homeland Security Newswire*, 2008), http://www.homelandsecuritynewswire.com/gaza-campaign-highlights-strength-limitations-air-power.

GEN Eade, George J., "Reflections of Air Power in the Vietnam War," *Air University Review*, Nov-Dec, 1973.

GEN Fogleman, Ronald R., "*Strategic Vision and Core Competencies*," delivered at the *Air Force Association Symposium*, Los Angeles, CA, 18 Oct 1996.

Hallion, Richard P., "Precision Guided Munitions and the New Era of Warfare," *Air Power Studies Centre*, APSC Paper n._53, 1995.

Kainikara, Sanu, "Future Employment of Small Air Forces," *RAAF Air Power Development Centre*, n._19, 2005.

LTC Chin, Pak Chuen, LTC Gan, Siow Huang, & MAJ Ng, Sin Kian, "Making a Difference: RSAF's Role in Peacetime Operations," *Pointer*, v._32 n._1, 2006.

LTC Tan, Yu Cherng; LTC Ng, Roland; and MAJ Foo, Chun Fai, "Transformation of Airpower," *Pointer*, v._30, n._3, 2004.

Mackenzie, S.A., *Strategic Air Power Doctrine for Small Air Forces*, Air Power Studies Centre, RAAF Base Fairbairn, Canberra, 1994.

MG Ng, Chee Khern, "Smaller Air Forces and the Future of Air Power – A Perspective from Singapore," *Pointer*, v._34, n._3, 2008.

Mitchell, William, *Winged Defense*, New York and London: G.P. Putnam's Sons, 1925.

"Psychological Operations in Support of Operation Restore Hope," (*Unified Task Force Somalia*, 1993), http://www.psywar.org/psywar/reproductions/OpRestoreHope.pdf.

Rodman, David, "The Role of the Israel Air Force in the Operational Doctrine of the Israel Defence Forces: Continuity and Change," http://www.airpower.maxwell.af.mil/airchronicles/cc/rodman.html.

Rothfels, H, "*Clausewitz*" *in Makers of Modern Strategy: Military thought from Machiavelli to Hitler*, ed. Edward Mead Earle, Princeton: Princeton University Press, 1971.

Warner, Edward, "Douhet, Mitchell, Seversky: Theories of Air Warfare," ed. Earle, E. M., *Makers of Modern Strategy, Princeton University Press*, 1973.

Weldes, Jutta, *Constructing National Interests – The United States and the Cuban Missile Crisis, Barrows Lectures*, 1999.

"Why US Airstrikes Have So Far Failed to Stop the Islamic State," (*The Washington Post*, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/10/06/why-u-s-airstrikes-have-so-far-failed-to-stop-the-islamic-state.

ENDNOTES

1. LTC Tan, Yu Cherng, LTC Ng, Roland and MAJ Foo, Chun Fai, "Transformation of Airpower," *Pointer*, v._30, n._3, 2004.

2. Douhet, Giulo, *The Command of the Air*, trans Dino Ferrari, Washington, D.C.: Office of Air Force History, 1983.

   Mitchell, William, *Winged Defense*, New York and London: G.P. Putnam's Sons, 1925, pp. 121-127.

3. GEN Eade, George J., "Reflections of Air Power in the Vietnam War," *Air University Review*, Nov-Dec, 1973.

   COL Hines, Anthony L., "Kosovo: The Limits of Air Power," *Air and Space Power Journal*, May 2002.

   "Gaza Campaign Highlights Strength, Limitations of Air Power," (Homeland Security *Newswire*, 2008), http://www.homelandsecuritynewswire.com/gaza-campaign-highlights-strength-limitations-air-power.

4. Examples of technological advances include Precision Guided Munitions, Network Centric systems and the proliferation of stealth capabilities.

5. GEN Fogleman, Ronald R., "Strategic Vision and Core Competencies," delivered at the Air Force *Association Symposium*, Los Angeles, CA, 18 Oct 1996.

6. MG Ng, Chee Khern, "Smaller Air Forces and the Future of Air Power – A Perspective from Singapore," *Pointer*, v._34, n._3, 2008.

7. Mackenzie, S.A., *Strategic Air Power Doctrine for Small Air Forces*, Air Power Studies Centre, RAAF Base Fairbairn, Canberra, 1994.

8. SAF definition of "deterrence": The preventing from action, such as preventing the initiation of armed action or inhibiting escalation if combat occurs, by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. This involves taking steps to convince the target being deterred that the costs involved in taking certain actions is higher than its expected benefits or the chance of success of his intended military actions is zero or negligible.

9. The SAF defines the strategic-level as follows: The level of war at which a state, often as a member of a group of states, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. Activities at this level establish national and multinational military objectives; sequence initiatives; define limits and assess risks for the use of military and other instruments of national power; develop global plans or theatre war plans to achieve those objectives; and provide military forces and other capabilities in accordance with strategic plans.

10. Garden, Timothy, "Air Power: Theory and Practice," in *Strategy in Contemporary World*, ed. Baylis, J.; Wirtz, J.; Cohen, E.; Gray, C.S., Oxford University Press, Chapter 6, 2002, pp. 155.

11. GEN Eade, George J., op.cit.

    COL Hines, Anthony L., op.cit.

12. "Gaza Campaign Highlights Strength, Limitations of Air Power," (*Homeland Security Newswire*, 2008), http://www.homelandsecuritynewswire.com/gaza-campaign-highlights-strength-limitations-air-power.

13. "Why US Airstrikes Have So Far Failed to Stop the Islamic State," (*The Washington Post*, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/10/06/why-u-s-airstrikes-have-so-far-failed-to-stop-the-islamic-state.

14. Winn, Gregory C., "Douhet: Still Relevant Today," (*USAF CSC, 1991)*, in http://www.globalsecurity.org/military/library/report/1991/WGC.htm.

15. Warner, Edward, "Douhet, Mitchell, Seversky: Theories of Air Warfare," ed. Earle, E. M., *Makers of Modern Strategy*, Princeton University Press, 1973, pp. 496-499.

    Futrell, Robert, F., *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force: 1907-1960*, v._1, Maxwell AFB: Air University Press, 1989, pp. 239.

16. Dayan, Uzi, "Air Power – The Israeli Perspective," *Military Technology*, v._23, n._5, May 1999.

17. Kainikara, Sanu, "Future Employment of Small Air Forces," *RAAF Air Power Development Centre*, n._19, 2005.

18. Egypt had by far the largest and the most modern of all the Arab air forces, consisting of about 420 combat aircraft, all of them Soviet-built and including top-of-the line MiG-21 capable of attaining Mach 2 speed. After the attack, a total of 338 Egyptian aircraft were destroyed and 100 pilots were killed. Among the Egyptian planes lost were all 30 Tu-16 bombers, as well as 27 out of 40 Il-28 bombers, 12 Su-7 fighter-bombers, over 90 MiG-21s, 20 MiG-19s, 25 MiG-17 fighters, and around 32 assorted transport planes and helicopters. The Israelis lost 19 planes, including two destroyed in air-to-air combat and 13 downed by anti-aircraft artillery.

19. Hallion, Richard P., " ", *Air Power Studies Centre*, APSC Paper n._53, 1995.

20. LTC Tan, Yu Cherng; LTC Ng, Roland; and MAJ Foo, Chun Fai, op.cit.

21. CPT Chen, Victor, "Rationalising the Paradigm Shift from Network-Centricity to Knowledge-Centricity," *Pointer*, v._36, n._1, 2010.

22. During the 2006 Lebanon War, Hezbollah militants launched over 4000 rockets into Israel, targeting and hitting dozens of cities. These were rockets were not advanced rockets, but crude Katyusha artillery rockets, each carrying warheads of about 30kg, with a range of 30km. Singapore, with a similar lack of strategic depth, shares the same vulnerability against such Rocket, Artillery and Mortar (RAM) threats.

23. Definition extracted from SAF dictionary: Early warning indicators are defined as items of information on military or other activities received by the intelligence agencies that is seen as a "telling sign" of military preparation by the target or his intention to go to war.

24. *Of which, a military blockade coupled with diplomatic pressure was the course of action taken to eventually diffuse the stand-off*. Ref: Weldes, *Jutta, Constructing National Interests – The United States and the Cuban Missile Crisis, Barrows Lectures*, 1999.

25. Rodman, David, "The Role of the Israel Air Force in the Operational Doctrine of the Israel Defence Forces: Continuity and Change," http://www.airpower.maxwell.af.mil/airchronicles/cc/rodman.html.

26. Chaim Herzog, *The Arab-Israeli Wars: War and Peace in the Middle East*, Second Vintage Books Edition, July 2005, p. 352.

27. "Psychological Operations in Support of Operation Restore Hope," (*Unified Task Force Somalia*, 1993), http://www.psywar.org/psywar/reproductions/OpRestoreHope.pdf.

    SAF Dictionary: PsyOps involves planned psychological activities directed at the enemy, friendly and neutral audiences in peace and war to influence their attitude and behaviour favourably to the achievement of political and military objectives. This may be:

    a. Battlefield psychological activities – Conducted as an integral part of combat operations against the enemy and civilians under enemy control in the battle area, to assist in achieving tactical objectives.

    b. Consolidation psychological activities – Conducted towards the civilian population located in areas under friendly control, to achieve a desired behaviour that supports the military objectives and operational freedom of supported commanders.

    c. Strategic psychological activities – Conducted to gain the support and cooperation of friendly and neutral countries, and to reduce the will and capacity of hostile or potentially hostile countries to wage war.

28. Rothfels, H, "*Clausewitz*" *in Makers of Modern Strategy: Military thought from Machiavelli to Hitler*, ed. Edward Mead Earle, Princeton: Princeton University Press, 1971, p. 102.

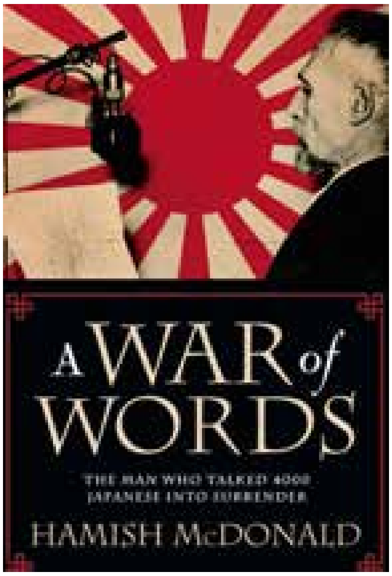
29. In foreign policy terms, hard power, mainly focusing on a state's military and economic power, emphasises the coercive aspect, where through coercion others are compelled to behave in a manner demanded by the coercer. On the other hand, soft power is the attempt to shape the behaviour of other states through attractions. While hard power focuses on the power to coerce, soft power emphasises on the power of persuasion.

30. MG Ng, Chee Khern, op.cit.

31. Chin Pak Chuen, Gan Siow Huang, & Ng Sin Kian, "Making a Difference: RSAF's Role in Peacetime Operations," *Pointer*, v._32 n._1, 2006.

LTC Victor Chen Kanghao is a UAV Pilot by vocation and is currently the Commanding Officer of UAV Training School. LTC Chen attended the Malaysian Armed Forces Command and Staff Course, where he received two awards, namely Best in Military Studies and Best Commandant's Paper. His previous appointments include Officer Commanding in 116 SQN and Staff Officer in SAF UAV Office, Air Plans Department. He holds a Master of Arts in Business Studies and Economics from the University of Edinburgh, United Kingdom, graduating with 1st Class Honours.

Book Review



Hamish McDonald, *A War of Words: The Man Who Talked 4000 Japanese into Surrender, (Queensland: University of Queensland Press), 2014, 332 pages.*

By **Jeria Kua**

INTRODUCTION

> "The War of Thought is as important as that of armed might or economy."
>
> *- Unknown Japanese army officer*[1]

In his latest book, author and journalist Hamish McDonald presents a riveting account of the extraordinary life of Charles Bavier – born a European but raised as a Japanese at the tumultuous turn of the 20th century. Set during a period of a rapidly-changing world order, this book traces Bavier's epic journey across Asia, including the 1911 Xinhai Revolution that ended 2,000 years of imperial rule in China, the Australia and New Zealand Army Corps' (ANZAC) 1915 Gallipoli Campaign, the British MI5's counter-intelligence operations in Southeast Asia, culminating in his indispensable role as a skilled propagandist for the Allies in World War Two's (WWII) Pacific Theatre. After over 30 years of research, McDonald has crafted an engaging historical narrative of a man whose *sui generis* cultural background enabled him to play an integral role in persuading an estimated 4,000 Japanese soldiers in the Southwest Pacific to surrender, and indirectly saving countless more lives. Through Bavier's story, readers are given an insight into the numerous trials and tribulations he faced in his quest for glory, as well as his unyielding desire to promote harmony between the two worlds of East and West.

AN EASTERN UPBRINGING

Charles Souza Bavier was born in January 1888 to a Swiss silk businessman Edouard de Bavier and his unknown European lover, amidst Japan's reopening of trade with the West after over 200 years of *sakoku*, or self-imposed isolation.[2] Abandoned by his biological parents immediately after birth, Bavier was entrusted to the care of his father's Japanese mistress in the port city of Yokohama. Over the next 20 years, he was brought up in a Japanese milieu under the name 'Sakai Hachisaburo,' and "never felt anything but Japanese until he was much older," with only his fair complexion and brown hair betraying his European heritage.[3]

From his early childhood, Bavier displayed a keen interest in military affairs and yearned for a career in the army. He read voraciously about famous military commanders and explorers like Napoleon and Columbus, practised *kendo* diligently, and drilled with the school cadet corps wherein he was appointed as a non-commissioned officer.[4] At the same time, his fascination with war and conflict mirrored the growing current of Japanese nationalism in society, which was intensified by the nation's decisive victory in the First Sino-Japanese War (1894-95) and its disputes with Russia over territorial claims in the Liaodong Peninsula. Militarism permeated the education of young men like Bavier, where they were taught to embody "the spirit of Japan's warlike ancestors," and that "the military were the expression of the national 'essence'."[5]

As the story begins to unfold, McDonald adroitly captures the zeitgeist of a nation craving for international prestige and imperial power through the careful use of language and evocative detail, despite the large amount of historical material covered. He is also able to induce feelings of sympathy on the part of the reader for Bavier and his estranged adoptive mother when he was neglected by his father, as well as reflect the tension between Bavier's Swiss ethnicity and the increasing distrust of foreigners in Japan, thus setting the stage for conflict.

ALIENATION AND REVOLUTION

Bavier's transition to adulthood in the first decade of the 20th century was no less fraught with suspense. Japan was engulfed in a bitter and protracted war with Russia from 1904-1905, fanning into flames the embers of anti-foreign, nationalistic sentiment all over the country. Indiscriminate attacks on foreigners were not uncommon, while the assassination of politicians seen capitulating to foreign powers was viewed as an act of loyalty to the emperor.[6] As the socio-political environment of Japan became darker and more chaotic, the author subtly criticises the corruption of the *bushido* spirit, now used as *carte blanche* for fanatical violence and racism.

Bavier himself, now an undergraduate student at the Waseda School of Commerce in Tokyo, had nearly fallen victim to one of these attacks during the Hibiya Riot of 5th September, 1905—a violent protest against the unsatisfactory peace treaty terms that concluded the war.[7] In what would prove to be a turning point in his life, he was rescued by the revolutionary activist Miyazaki Toten, a close aide of Sun Yat-sen, and became immersed in the Chinese revolutionary movement growing in Tokyo. With his thirst for adventure and military glory stirred, he attended the meetings of the radical socialist elements in the city and joined the *Tongmenghui*, a revolutionary body dedicated to overthrowing the Manchu rule in China. Believing in his calling to be on the battlefield, he left school and set sail for China.

Caught in the throes of military uprising and political upheaval, the late Qing Dynasty China was truly a kaleidoscope of conflict and turmoil. Due to the chaotic nature of this period, McDonald manipulates the flow of time in the narrative, speeding it up and slowing it down to emphasise key events, thus sustaining the reader's interest. Bavier travelled from city to city, helping to garner logistical support for the insurgency and assisting communication among the various revolutionary groups. He joined a medical team bringing Chinese casualties out of Hanyang, gave tuition in the Japanese and English languages, drilled with the international volunteer corps, and was nearly involved in an assassination attempt on Yuan Shikai, the commander of the Beiyang Army and Prime Minister of Imperial China.[8] Despite the success of the revolution in 1911, Bavier failed to gain any recognition for his contributions. Disappointed but not dispirited, he set out to "fulfil the destiny he felt was waiting" in the newly-formed ANZAC.[9]

IN THE TRENCHES OF GALLIPOLI: FIGHTING WITH THE ANZAC

Military glory, however, would once again elude Bavier in the miserable, plague-infested trenches of Lone Pine. Characteristic of many of the battles fought during World War One (WWI), the Australians failed to gain significant ground against the Turks during the 1915 Gallipoli Campaign and a fruitless stalemate ensued. Obvious to him that he was on the losing side, the freshly-minted Sergeant felt disillusioned with the Allied commanders' lack of strategic depth and their failure to use the element of surprise to their advantage—a tactic stressed upon during his studies of Sun Tzu and Clausewitz. Raising this to his superiors, he was accused of spreading disaffection among the soldiers and was harshly upbraided.[10] Nor would his unique background endear himself to his fellow men and officers. Australia at that time was deeply fearful of enemy spies and especially Japan, which had altered the regional balance of power following the 1902 Anglo-Japanese Treaty of Alliance.[11] Bavier himself was suspected of being an informant for the Japanese and was regarded with distrust. A laceration to his face after merely 3 weeks in combat was what delivered the *coup de grace* to his military career, sending him back to Japan with nothing but shame.

SWITCHING SIDES

Back in his homeland, a new wave of change had enveloped the nation. The boom years of WWI had spread affluence and prosperity among the urban middle class in Japan, driving consumerism and a voracious appetite for all things Western.[12] Now in his thirties with his thirst for adventure cooled, Bavier began to settle down and seek a stable life. He married a Japanese woman in 1920 and flourished briefly as an English teacher and foreign expert. He even enjoyed the status of a minor celebrity, writing articles on Japanese culture for newspapers, giving broadcast talks over the radio and appearing on public discussions.[13] As always, the author's use of vibrant imagery helps draw readers into the fevered atmosphere of cultural experimentation and dynamism, as well as its precipitous decline following the Great Kanto Earthquake of 1st September, 1923.

The sheer carnage wrought by the disaster shook the public mood and exposed the deep fissures within society. People found scapegoats in Koreans and the radical elements in the city, while feelings of fear and confusion were manipulated by ultra-nationalistic conservatives within the military sphere. Compounded by the Great Depression in 1929, the assassinations and fanatical violence of the first decade returned. Japan became increasingly isolationist. Public sentiment began to turn against Bavier too, who received threats and was constantly kept under surveillance by the secret police.

The increasingly hostile state of affairs saw him and his family flee firstly to Hong Kong, and then colonial Singapore in 1938, where he eventually found work under Colonel Hayley Bell, the head of station for the MI5. Disturbed by Japan's growing militarism with the outbreak of war in China, Bavier operated as an undercover agent for the British, gathering intelligence about Japanese movements in Singapore under the guise of an education consultant to Raffles College. In what would foreshadow his future role in ending the war, he also worked as a propagandist under the Information Ministry, broadcasting commentaries exaggerating Singapore's defences with the aim of sowing doubt in the Japanese minds about attacking the British naval base.

Of particular interest to readers would be McDonald's account of the fall of Singapore, considered then to be an impregnable military fortress. Although Bavier had personally uncovered the Japanese strategy of a *blitzkrieg*-like attack from the Malayan peninsula rather than a naval battle, hubris and complacency had permeated the top brass of military officials. Despite his team's efforts in pointing out Singapore's vulnerability, Colonel Bell was admonished for "causing unnecessary alarm and weakening morale," and was eventually replaced.[14] By the time the British finally began strengthening the island's defences, it was too little and too late.

A WAR OF WORDS

Impressed by his achievements in the MI5, Bavier was recruited to join the new Far Eastern Liaison Office (FELO) in Brisbane, the military propaganda section of the Allied Intelligence Bureau.[15] With the war in the Pacific now in full swing, he thus began his 3-year long assault on Japanese morale. Inspired by Sun Tzu's precept of achieving victory without fighting by dispiriting the enemy's troops ahead of battle, Bavier pioneered a new line of propaganda playing on the Japanese soldiers' feelings of nostalgia and homesickness. He and his team designed and air-dropped leaflets containing nostalgic scenes of home, reminding them of loved ones eagerly awaiting their safe return. FELO units were also sent to the frontlines to broadcast Bavier's pre-recorded exhortations to surrender, the oral testimonies of Japanese prisoners, and even traditional music from home. The impact of the propaganda campaign was tangible: the stream of prisoners gradually rose, many of whom attested their motivation to surrender to the FELO leaflets. Bavier's broadcasts had reportedly disturbed Japanese authorities so much that they banned their soldiers from listening.[16] By the end of the war, 4,160 Japanese soldiers were saved as a result of FELO's efforts, not including the countless Allied lives they might have taken if they had persisted fighting.[17]

So what was Bavier's significance in all of this? It was his masterful command of the Japanese language, deep cultural penetration and knack for military strategy that allowed him to craft the leaflets and broadcasts persuading these soldiers to think about an alternative to blind sacrifice to their emperor and nation.[18] Although there were many second-generation Japanese-Americans working for FELO who were fluent in the language, they were already "Americans in a Japanese skin," lacking the literary skills and vernacular to connect culturally with the Japanese audience.[19] It was ultimately Bavier who added authenticity to FELO's propaganda campaign and propelled its success.

Yet, Bavier was not alone in the fight. He was joined by an eclectic crew of linguists, intelligence experts, military personnel and even defected soldiers from the Japanese Army who had a vital role to play in the conceptualisation of the FELO leaflets. Even the final figure of roughly 4,000 Japanese soldiers who surrendered was attributed to FELO as a whole and not solely to Bavier. It is therefore important to recognise that the propaganda campaign was fundamentally a team effort.

McDonald's portrayal of the Allied propaganda war with Japan gives us a valuable insight into one of the less documented battlefields of WWII. Underneath the dehumanised and vicious fighting, we learn that these soldiers were all fundamentally human, each with their own unique background, hopes and ambitions. Bavier's story encourages us to appreciate our similarities instead of focusing on our differences. With his life spent caught between the two worlds of East and West, he is no doubt a living testimony to inter-cultural peace.

CONCLUSION

It is easy to view Charles Bavier as a tragic and flawed character. He was abandoned by his biological family, alienated by the country he grew up in, and regarded as a spy by the Allied Forces. His aspirations of a glorious military career ended in ignominy, both in revolutionary China and the trenches of Gallipoli. Moreover, he was described by his stepson as an "inveterate philanderer," who possessed numerous sexual relationships during his early days and an extramarital affair later.[20]

Yet, in the final assessment, what can we learn from Bavier's long and eventful life? Despite his numerous setbacks and ostracism as a "yellow man inside a white skin," Bavier always looked beyond his present circumstances, and sought to use his literary skills and deep understanding of the Japanese psyche "to preach that better mutual understanding would lessen the tensions between Japan and the Western powers," and to "educate the Western nations about the depth of (Japan's) culture and artistic accomplishments."[21]

Or perhaps, it was precisely because of his unique upbringing, coupled with his strength of character, that he was able to prevail in the hour of need as the bridge between the East and West, as exemplified by his role in the saving of thousands of Japanese lives in WWII that would have been lost for naught.

The book is not without its criticisms, however. McDonald employs a novelistic manner of storytelling, which although enriches the narrative may compel readers to question its veracity. Bavier's attempted autobiography, the main source of material for McDonald, contained "scraps of biographical anecdotes (that) came in no particular order," meaning that certain conversations and scenes had to be imagined from the author's point of view rather than based on Bavier's own testimony.[22] For example, in depicting colonial Singapore in the 1930s, McDonald pictured "glossy blue-black crows (clawing) and (jostling) in a frangipani tree covered in white flowers...From a bamboo cage hanging on the verandah, a large black bird with a bright yellow beak and wattle let out a piercing shriek."[23] While this helps to inject life and colour into Bavier's world and fill in the gaps in his story, it is dramatised to some extent. For a man who kept much of his life a secret, perhaps we should exercise due caution when reading this book.

Overall, *A War of Words* remains an enjoyable read and is highly recommended for those who wish to gain an insight into the psychological dimension of war, as well as the complex relationships among the disparate nations of Asia during the early 20th century. 🌏

ENDNOTES

1. Gilmore, Allison B., *You Can't Fight Tanks with Bayonets: Psychological Warfare against the Japanese Army in the South West Pacific* (Lincoln, Nebraska: University of Nebraska Press, 1998), 9.

2. McDonald, Hamish, *A War of Words: The Man Who Talked 4000 Japanese into Surrender* (Queensland: University of Queensland Press, 2014), 13.

3. Ibid., 20.

4. Ibid., 52, 46

5. Ibid., 55.

6. Ibid.

7. "Social Protest in ImperialJapan: *The Hibiya Riot of 1905*", (MIT Visualizing Cultures, 2011), http:/ocw.mit.edu/ans7870/21f/21f.027 social_protest_japan/index.html.

8. Michael Yang, "Yuan Shikai", (*China Highlight*s, 2015), http://www.chinahighlights.com travelguide/china-history/yuan shikai.htm.

9. McDonald, Hamish, *A War of Words: The Man Who Talked 4000 Japanese into Surrender* (Queensland: University of Queensland Press, 2014), 121.

10. Ibid., 141.

11. Ibid., 122, 125.

12. Ibid., 154.

13. Ibid., 156.

14. Ibid., 214.

15. Peter Dunn, "Far Eastern Liaison Office (FELO) Military Propaganda Section: Section "D" of Allied Intelligence Bureau (AIB) in Australia During WW2", (*Australia@ War*: 2006), http://www.ozatwar.com/sigint/felo.htm.

16. McDonald, Hamish, *A War of Words: The Man Who Talked 4000 Japanese into Surrender* (Queensland: University of Queensland Press, 2014), 336.

17. Ibid., 275.

18. Ibid., 315.

19. Ibid., 250.

20. Ibid., 311.

21. Ibid., 82, 198, 152.

22. Ibid., 7.

23. Ibid., 196.

Brigadier General William Billy Mitchell (1879-1936)

by **Macalino Minjoot**

> *"With us air people, the future of our nation is indissolubly bound up in the development of air power."*
>
> *- Brigadier General William Billy Mitchell*[1]

INTRODUCTION

Brigadier General William Billy Mitchell was a man who saw the future of air power. A determined and intelligent soldier, he pushed authorities to the limits in order to prove his point. His 'radical' ideas included using fighter planes, instead of battle ships, and soldiers transported by air and not just through land.

EARLY LIFE

William Billy Mitchell was born on 29th December 1879, in Nice, France to John Lendrum Mitchell, a wealthy Wisconsin senator and Harriet Michelle.[2] Mitchell was the eldest of his nine other siblings and came from a distinguished family. His grandfather Alexander Mitchell, a Scotsman, was the wealthiest person in Wisconsin at his time and established what became the Milwaukee Road railroad and the Marine Bank of Wisconsin. Mitchell Park and the shopping precinct of Mitchell Street were named in honor of Alexander.

Mitchell and his siblings learned German, Italian and Spanish. He also spoke French as fluently as English.

Mitchell's father was elected to Congress in 1891 and to the Senate in 1893. Important guests were often invited to the Mitchell home and, the children were encouraged to interact and converse with their parents' guests. Mitchell was allowed at the dinner table with important guests, and always found a way to participate in the conversations.[3]

Mitchell graduated from Columbian College of George Washington University in 1898.

CAREER AND INTEREST IN AVIATION

In May 1898, Mitchell enlisted at age of 18 in the Army as a private in Company M of the 1st Wisconsin Infantry Regiment when the Spanish-American War broke out. He was commissioned and served in the Army Signal Corps in Cuba, the Philippines and Alaska before becoming interested in aviation.[4]

Mitchell was sent to Alaska in 1901 where he successfully built telegraph lines in remote areas. During this posting, he began studying Otto Lilienthal's glider experiments. This reading, combined with further research, led him to conclude in 1906 that future conflicts would be fought in the air.[5]

In March 1912, Mitchell was assigned to the Army General Staff in Washington in 1912 as a captain. At the age of 32, he was the youngest out of the 21 officers selected to serve the General Staff.

In 1913, Mitchell was sent to the Army Staff College and became the only Signal Corps Officer on the Army General Staff.[6] As aviation was assigned to the Signal Corps, Mitchell was well placed to further develop his interest.[7] He was chosen as temporary head of the Aviation Section, U.S. Signal Corps, predecessor of the modern United States (US) Air Force.

In 1916, Mitchell was made Deputy Commander of the Aviation Section, Signal Corps. The US Army felt that Mitchell, at the age of 38, was too old for flying lessons. Hence, he was forced to seek private instruction at the Curtiss Aviation School in Newport News where he managed to pick up this skill quickly.[8]

WORLD WAR I

On 6th April, 1917, the US declared war on Germany and Mitchell, by then a Lieutenant Colonel, headed towards France as an observer. He immediately went to Paris and set up an office. In Paris, he learned how to develop aerial combat strategies and planned large-scale air operations when working closely with the Royal Flying Corps' General Sir Hugh Trenchard.

In two weeks, he became the first American officer to fly over the lines when he rode with a French pilot. Mitchell quickly earned a reputation as a daring and tireless leader. He was promoted to Brigadier General and given command of all American air units in General John J. Pershing's American Expeditionary Force. Slowly, more American pilots arrived and they piloted French planes.

On Sunday, 14th April, 1918, a year after the US entered the war, Mitchell declared that America had finally put its first squadron into combat. His flair for combat leadership was subsequently proven at the Battle of Saint-Mihiel when he co-ordinated a force of 1,481 British, French and Italian planes, to support American ground forces. During his time in France, Mitchell proved a highly effective commander, but his aggressive approach and unwillingness to operate in the chain of command made him numerous enemies.

For his performance in World War One (WWI), Mitchell received several awards which includes; the Distinguished Service Cross, the Distinguished Service Medal, the World War I Victory Medal with eight campaign clasps and several foreign decorations.

POST WORLD WAR I

Mitchell returned to the US as a hero in 1919 and was appointed Assistant Chief of the US Army Air Service. He was appalled at how quickly the organisation he had helped to build in war had disintegrated in peacetime.

AIR ADVOCATE

Mitchell was supposed to have the post-war assignment of Director of Air Service after the leadership he portrayed in WWI.

However, Major General Charles T. Menoher, an artilleryman who had commanded the 42nd 'Rainbow' Division in France, was appointed Director instead, on the recommendation of his classmate General Pershing, to maintain operational control of aviation by the ground forces.[10] This appointment surprised many who felt that Mitchell was more suited for that position.

Mitchell was able to retain his wartime rank of Brigadier General. A relentless advocate for aviation, he encouraged US Army Air Force pilots to challenge records, as well as promoted races, and ordered aircraft to aid in fighting forest fires. Convinced that air power would become the driving force of war in the future, he pressed for the creation of an independent Air Force.

However, Mitchell the war hero soon became known as Mitchell the Agitator. Mitchell's vocal support of air power brought him into conflict with the US Navy as he felt that the importance of an Air Force would make Navies' battleships increasingly obsolete. He tried to prove that airplanes could actually accomplish the things he had said. He then proposed a number of daring innovations for the Air Service that stunned the non-flying Army generals—a special corps of mechanics, troop-carrying aircraft, a civilian pilot pool for wartime availability, long-range bombers capable of flying the Atlantic and armor-piercing bombs. Convinced that bombers could sink battleships, he argued that aviation should be the US's first line of defence. He encouraged the development of bombsight, ski-equipped aircraft, engine superchargers, aerial torpedoes and the concept of Airborne, an idea that allowed troops to parachute from airplanes to land in the amidst of a battlefield. He ordered the establishment of aerial forest-fire and border patrols and followed that with a mass flight to Alaska, a transcontinental air race and a flight around the perimeter of the US. He also encouraged Army pilots to set speed, endurance and altitude records at all cost in order to keep aviation in the news.

With each success, Mitchell became more determined that the nation's money should be spent on aircraft and not on expensive battleships. He stepped on the egos of Army generals and Navy admirals with his fiery way of words and boasted that Army planes could sink any battleship afloat under any conditions of war. Dynamic and impulsive, Mitchell sought out the American press and announced that if he were given permission to bomb captured German battleships, he would be able to prove his assertions.

Among those he alienated was Assistant Secretary of the Navy, Franklin D. Roosevelt. Failing to achieve his goals, Mitchell became increasingly outspoken and attacked his superiors in the US Army, as well as the leadership of the US Navy and White House for failing to understand the importance of military aviation.

PROJECT B

In February 1921, Mitchell was anxious to test his theories of destruction of ships by aerial bombing. Reluctantly, both Secretary of War, Newton Baker and Secretary of the Navy, Josephus Daniels agreed to a series of joint Army-Navy exercises to be held that summer in which captured ships could be used as targets. Mitchell believed that he could succeed in 'wartime conditions', and that a thousand bombers could be built for the price of one battleship, making aviation a more economical defence force.[11]

Dubbed Project B, the exercises were moved forward to June and July 1921 under a set of rules of engagement that greatly favored the survivability of the ships. In the early tests, Mitchell's aircraft sank a captured German destroyer and light cruiser. From 20th – 21st July, they attacked the German battleship *Ostfriesland*.[12] However, Mitchell violated the rules of engagement by sinking the battleship. In addition, the circumstances of the exercises were not under 'wartime conditions' as all of the target vessels were stationary and effectively defenseless at that point of time.

FALL FROM POWER

Mitchell repeated his success later that year by sinking the retired battleship USS *Alabama* in September. The tests provoked President Warren Harding who wished to avoid any show of naval weakness immediately prior to the Washington Naval Conference. However, the sinking of the retired battleship USS *Alabama* did lead to increased funding for military aviation.

Mitchell continued to criticise his superiors regarding aviation policy. In 1924, the commander of the Air Service, Major General Mason Patrick, sent him on a tour of Asia and the Far East to remove him from the limelight. During this tour, Mitchell foresaw a future war with Japan and predicted an aerial attack on Pearl Harbor. That fall, he again blasted the Army and Navy leadership, this time to the Lampert Committee. The following March, his term of Assistant Chief ended and he was exiled to San Antonio, Texas with the rank of Colonel, to oversee air operations.

COURT MARTIAL

Later that year, following the loss of the US Navy airship USS *Shenandoah*, Mitchell issued a statement accusing the military's senior leadership of 'almost treasonable administration of the national defense' and incompetence. As a result of these statements, he was brought up on court-martial charges for insubordination at the direction of President Calvin Coolidge. Beginning that November, the court-martial saw Mitchell receive broad public support and notable aviation officers such as Eddie Rickenbacker, Henry Arnold and Carl Spaatz testifying on his behalf.[13]

On 17th December, 1925, Mitchell was found guilty and sentenced to a five-year suspension from active duty and loss of pay. The youngest of the twelve judges, Major General Douglas MacArthur, called serving on the panel 'distasteful', and voted not guilty stating that an officer should not be "silenced for being at variance with his superiors in rank and with accepted doctrine."[14] Rather than accept the punishment, Mitchell resigned on 1st February, 1926.

LATER LIFE

Mitchell wrote more than 60 articles, several newspaper series and five books, never deviating from his appeal for public understanding of the promise and the potential of air power. He made his last public appearance on 11th February, 1935, when he addressed the House Military Affairs Committee.

Weakened by his struggle, the old campaigner died in a New York hospital on 19th February, 1936, at the age of 56. He had elected to be buried in Milwaukee, his hometown, where he enlisted in 1898, rather than at Arlington National Cemetery.

CONCLUSION

Mitchell not only foresaw that an Air Force was essential for national survival, he also educated the public and its leaders on the role that air power would eventually play in national defence. For his foresight and willingness to sacrifice his career for his beliefs, the US owes this visionary man a debt of gratitude it can never repay. Many wondered if he was successful in becoming the Chief of Air Force at the earliest stage, what other plans or theories he could have implemented.

ENDNOTES

1. Brainy Quote. http://www.brainyquote.com/quotes/authors/b/billy_mitchell.html

2. The United States Senate is a legislative chamber in the bicameral legislature of the United States, and together with the House of Representatives makes up the U.S. Congress.

   Wikipedia. https://en.wikipedia.org/wiki/United_States_Senate

3. Biography. http://biography.yourdictionary.com/billy-mitchell

4. Military Aviation: Brigadier General Billy Mitchell. http://www.historynet.com/william-billy-mitchell-an-air-power-visionary.htm

5. Ibid.

6. Billy Mitchell, Crusader for Air Power, Alfred F. Hurley. 17.

7. Ibid.

8. Military Aviation: Brigadier General Billy Mitchell. http://militaryhistory.about.com/od/airforce/p/Military-Aviation-Brigadier-General-Billy-Mitchell.htm.

9. Colonel Phillip S. Meilinger, USAF. Maxwell AFB. American Airpower Biography: Billy Mitchell. http://www.au.af.mil/au/404.asp.

10. Major General Charles T. Menoher. Biography. https://en.wikipedia.org/wiki/Charles_T._Menoher.

    Hakim, Joy (1995). A History of Us: War, Peace and all that Jazz. New York: Oxford University Press.

11. Project B. https://en.wikipedia.org/wiki/Billy_Mitchell#Project_B:_Anti-ship_bombing_demonstration

12. General William “Billy” Mitchell and the Sinking of the Ostfriesland: A Consideration. http://blog.nasm.si.edu/aviation/general-william-%E2%80%9Cbilly%E2%80%9D-mitchell-and-the-sinking-of-the-ostfriesland-a-consideration/

13. Eddie Rickenbacker an American fighter ace in World War I and Medal of Honor recipient. With 26 aerial victories, he was America's most successful fighter ace in the war. https://en.wikipedia.org/wiki/Eddie_Rickenbacker

    Henry Harley "Hap" Arnold was an American general officer holding the grades of General of the Army and General of the Air Force. https://en.wikipedia.org/wiki/Henry_H._Arnold

    Carl Andrew "Tooey" Spaatz was an American World War II general. As commander of Strategic Air Forces in Europe in 1944, he successfully pressed for the bombing of the enemy’s oil production facilities as a priority over other targets. https://en.wikipedia.org/wiki/Carl_Andrew_Spaatz

14. MacArthur 1964, 85.

Quotable Quotes

It is good to be ambitious. It is because of ambition that Singapore progressed as quickly as we did. But ambition must be backed by hard work and solid skill.
– Lee Hsien Loong (b.1952), Prime Minister of Singapore.

Even peace may be purchased at too high a price.
- Benjamin Franklin (1705-1790), one of the Founding Fathers of the United States

Necessity is the mother of invention.
- Plato (c.427-347 BC), Greek philosopher

Let us not pray to be sheltered from dangers but to be fearless when facing them.
- Rabindranath Tagore (1861-1941), Indian poet

One minute decides the outcome of a battle, one hour the success of a campaign, one day the fate of empires
- Alexander Suvorov (1729-1800), undefeated Russian military leader and national hero

War is what happens when language fails.
- Margaret Atwood (b.1939), Canadian novelist, poet and literary critic

Individual commitment to a group effort—that is what makes a team work, a company work, a society work, a civilisation work.
- Vince Lombardi (1913-1970), American football player and coach

Plans are only good intentions unless they immediately degenerate into hard work.
- Peter Drucker (1909-2005), American management consultant, educator and author

We should not fret for what is past, nor should we be anxious about the future; men of discernment deal only with the present moment.
- Chanakya (c.370-283 BC), Indian teacher, philosopher and royal advisor

The things that have been most valuable to me, I did not learn them in school.
- Will Smith (b.1968), American actor and producer

However difficult life may seem, there is always something you can do and succeed at.
- Stephen Hawking (b.1942), British scientist and author

All of us every single year, we are a different person. I don't think we are the same person all our lives.
- Steven Spielberg (b.1946), American director, producer and screenwriter

He who wishes to be obeyed must know how to command.
- Niccolo Machiavelli (1469-1527), Italian philosopher, politician, and writer

Do not seek to follow in the footsteps of the wise. Seek what they sought.
- Matsuo Basho (1644-1694), Japanese poet

Coming together is a beginning; keeping together is a progress; working together is success.
- Henry Ford (1863-1947), American industrialist and founder of Ford Motor Company

Peace cannot be kept by force. It can only be achieved by understanding.
- Albert Einstein (1879-1955), theoretical physicist

Management is doing things right; leadership is doing the right things.
- Peter Drucker (1909-2005), educator and author

Progress is impossible without change, and those who cannot change their minds cannot change anything.
- George Bernard Shaw (1856-1950), Irish playwright, critic and polemicist

An investment in knowledge pays the best interest.
- Benjamin Franklin (1705-1790), one of the Founding Fathers of the United States

You will never win if you never begin.
- Helen Rowland (1875-1950), American journalist and humourist

What happens is not as important as how you react to what happens.
- Ellen Glasgow (1873-1945), American novelist

War is never a lasting solution for any problem.
- A. P. J. Abdul Kalam (1931-2015), 11th President of India

Courage is contagious. When a brave man takes a stand, the spines of others are often stiffened.
- Billy Graham (b.1918), American Christian evangelist

A leader is one who knows the way, goes the way, and shows the way.
- John Maxwell (b.1947), American author, speaker, and pastor

Love and compassion are necessities, not luxuries. Without them humanity cannot survive.
- Dalai Lama (b.1935)

Innovation distinguishes between a leader and a follower.
- Steve Jobs (1955-2011), American entrepreneur and inventor, co-founder of Apple Inc.

Weapons are like money; no one knows the meaning of enough.
- Martin Amis (b.1949), British writer

No man will make a great leader who wants to do it all himself, or to get all the credit for doing it.
- Andrew Carnegie (1835-1919), Scottish-American businessman and philanthropist

Instructions for Authors

AIMS & SCOPE

POINTER is the official journal of the Singapore Armed Forces. It is a non-profit, quarterly publication that is circulated to MINDEF/SAF officers and various foreign military and defence institutions. POINTER aims to engage, educate and promote professional reading among SAF officers, and encourage them to think about, debate and discuss professional military issues.

SUBMISSION DEADLINES

All articles submitted are reviewed on a rolling basis. The following dates indicate the approximate publication dates of various issues:

No. 1 (March)
No. 2 (June)
No. 3 (September)
No. 4 (December)

SUBMISSION GUIDELINES

POINTER accepts the contribution of journal articles, book reviews and viewpoints by all regular/NS officers, military experts and warrant officers. POINTER also publishes contributions from students and faculty members of local/international academic institutions, members of other Singapore Government Ministries and Statutory Boards, as well as eminent foreign experts.

Contributors should take note of pertinent information found in the Author's Guide when preparing and submitting contributions.

Article Topics

POINTER accepts contributions on the following topics:

- Military strategy and tactics
- SAF doctrinal development and concepts
- Professionalism, values and leadership in the military
- Military Campaigns or history and their relevance to the SAF
- Personal experiences or lessons in combat operations, peace-keeping operations or overseas training
- Defence management, administration and organisational change issues
- Defence technology
- Warfighting and transformation
- Leadership
- Organisational Development
- Conflict and Security Studies

Book Reviews

POINTER accepts reviews of books under the SAF Professional Reading Programme and other suitable publications. Contributors may review up to four books in one submission. Each review should have 1,500 - 2,000 words.

Viewpoints

Viewpoints discussing articles and those commenting on the journal itself are welcome. *POINTER* reserves the right for contents of the viewpoints to be published in part or in full.

Required Information

Manuscripts must be accompanied by a list of bio-data or CV of the author detailing his/her rank, name, vocation, current unit & appointment, educational qualifications, significant courses attended and past appointments in MINDEF/SAF.

Upon selection for publication, a copy of the "Copyright Warranty & License Form" must be completed, and a photograph of the author (in uniform No. 5J for uniformed officers and collared shirt for others) must be provided.

Submission of Manuscript

The manuscript should be submitted electronically, in Microsoft Word format, to **pointer@defence.gov.sg.**

Article Length

Each article should contain 2,000 to 4,000 words.

ENDNOTE FORMAT

Author's Responsibilities

Authors are responsible for the contents and correctness of materials submitted. Authors are responsible for:

- the accuracy of quotations and their correct attribution
- the accuracy of technical information presented
- the accuracy of the citations listed
- the legal right to publish any material submitted.

Endnotes

As with all serious professional publications, sources used and borrowed ideas in POINTER journal articles must all be acknowledged to avoid plagiarism.

Citations in POINTER follow the *Chicago Manual of Style.*

All articles in *POINTER* must use endnotes. Note numbers should be inserted after punctuation. Each endnote must be complete the first time it is cited. Subsequent references to the same source may be abbreviated.

The various formats of endnotes are summarized below. Punctuate and capitalise as shown.

Books

Citations should give the author, title and subtitle of the book (italicised), editor or translator if applicable (shortened to 'ed.' or 'trans.'), edition number if applicable, publication information (city, publisher and date of publication), appropriate page reference, and URL in the case of e-books. If no author is given, substitute the editor or institution responsible for the book.

For example:

Tim Huxley, *Defending the Lion City: The Armed Forces of Singapore* (St Leonard, Australia: Allen & Unwin, 2000), 4.

Huxley, *Defending the Lion City,* 4.

Ibid., 4.

Edward Timperlake, William C. Triplett and William II Triplet, *Red Dragon Rising: Communist China's Military Threat to America* (Columbia: Regnery Publishing, 1999), 34.

Articles in Periodicals

Citations should include the author, title of the article (quotation marks), title of periodical (italicised), issue information (volume, issue number, date of publication), appropriate page reference, and URL in the case of e-books. Note that the volume number immediately follows the italicised title without intervening punctuation, and that page reference is preceded by a colon in the full citation and a comma in abbreviated citations.

For example:

> Chan Kim Yin and Psalm Lew, "The Challenge of Systematic Leadership Development in the SAF," *POINTER* 30, no. 4 (2005): 39-50.
>
> Chan and Lew, "The Challenge of Systematic Leadership Development in the SAF," 39-50.
>
> Ibid., 39-50.
>
> Mark J. Valencia, "Regional Maritime Regime Building: Prospects in Northeast and Southeast Asia," *Ocean Development and International Law* 31 (2000): 241.

Articles in Books or Compiled Works

> Michael I. Handel, "Introduction," in *Clausewitz and Modern Strategy,* ed. Michael I. Handel, (London: Frank Cass, 1986), 3.
>
> H. Rothfels, "Clausewitz," in *Makers of Modern Strategy: Military thought from Machiavelli to Hitler,* eds. Edward Mead Earle and Brian Roy, (Princeton: Princeton University Press, 1971), 102.

Articles in Newspapers

Citations should include the author, title of the article (quotation marks), title of newspaper (italicised), date of publication, appropriate page reference, and URL in the case of e-books.

For example:

> David Boey, "Old Soldiers Still Have Something to Teach," *The Straits Times,* 28 September 2004, 12.
>
> Donald Urquhart, "US Leaves it to Littoral States; Admiral Fallon Says Region Can Do Adequate Job in Securing Straits," *The Business Times Singapore,* 2 April 2004, 10.

Online Sources

Citations should include the author, title of the article (quotation marks), name of website (italicised), date of publication, and URL. If no date is given, substitute date of last modification or date accessed instead.

For example:

> Liaquat Ali Khan, "Defeating the IDF," *Counterpunch,* 29 July 2006, http://www.counterpunch.org/khan07292006.html.

If the article was written by the publishing organisation, the name of the publishing organisation should only be used once.

For example:

> International Committee of the Red Cross, "Direct participation in hostilities," 31 December 2005, http://www.icrc.org/Web/eng/siteeng0.nsf/html/participation-hostilities-ihl-311205.

If the identity of the author cannot be determined, the name of the website the article is hosted on should be used. For example:

> "Newly unveiled East Jerusalem plan put on hold," *BBC News,* 2 March 2010, http://news.bbc.co.uk/2/hi/middle_east/8546276.stm.

More details can be found at **http://www.mindef.gov.sg/imindef/publications/pointer/contribution/authorsguide.html.**

EDITORIAL ADDRESS

Editor, POINTER
AFPN 1451
500 Upper Jurong Road
Singapore 638364
Tel: **6799 7755**
Fax: **6799 7071**
Email: pointer@defence.gov.sg
Web: www.mindef.gov.sg/safti/pointer

COPYRIGHT

All contributors of articles selected for POINTER publication must complete a "Copyright Warranty & License Form." Under this agreement, the contributor declares ownership of the essay and undertakes to keep *POINTER* indemnified against all copyright infringement claims including any costs, charges and expenses arising in any way directly or indirectly in connection with it. The license also grants POINTER a worldwide, irrevocable, non-exclusive and royalty-free right and licence:

- to use, reproduce, amend and adapt the essay, and
- to grant, in its sole discretion, a license to use, reproduce, amend and adapt the essay, and to charge a fee or collect a royalty in this connection where it deems this to be appropriate.

The "Copyright Warranty & License Form" is available at **http://www.mindef.gov.sg/imindef/publications/pointer/copyright/copyright.html.**

REPRINTS

Readers and authors have free access to articles of *POINTER* from the website. Should you wish to make a request for the reproduction or usage of any article(s) in POINTER, please complete the following "Request for Reprint Form" and we will revert to you as soon as possible available at **http://www.mindef.gov.sg/imindef/publications/pointer/copyright/requestform.html.**

PLAGIARISM

POINTER has a strict policy regarding such intellectual dishonesty. Plagiarism includes using text, information or ideas from other works without proper citation. Any cases of alleged plagiarism will be promptly investigated. It is the responsibility of the writer to ensure that all his sources are properly cited using the correct format. Contributors are encouraged to consult the NUS guidelines on plagiarism, available at **http://www.fas.nus.edu.sg/undergrad/toknow/policies/plagiarism.html.**

POINTER

The Journal of the Singapore Armed Forces

ISSN 2017-3956

pointer

Vol. 42 No. 3 [2016]

THE JOURNAL OF THE SINGAPORE ARMED FORCES