POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

Vol. 43 No. 2 [2017]

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© 2017 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.

POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

ISSN 2017-3956

Vol. 43 No. 2 [2017]

contents

contents

BOOK REVIEW

PERSONALITY PROFILE

QUOTABLE QUOTES

Editorial

In this issue of Pointer, we are pleased to present our top three prize-winning essays from the 2015/2016 Chief of Defence Force Essay Competition (CDFEC). Our top prize-winning essay, entitled 'Finding SAF's Place in the Cyber Age' is by MAJ Sebestian Xu. MAJ Xu highlights that as cyber space can no longer be ignored and is now widely recognised as a fast-expanding domain of modern warfare, militaries around the world are faced with a very serious threat they need to grapple with. This can be seen from the escalating frequency and devastating scale of cyber attacks in recent years—even countries such as Russia and the United States (US) have fallen victim to cyber attacks. MAJ Xu emphasises that because of the nature of cyber attacks, the rules that generally govern modern warfare in domains such as land, air, sea and space will not apply in the cyber domain. As Singapore becomes increasingly connected and cyber operations become increasingly sophisticated, MAJ Xu feels that the Singapore Armed Forces (SAF) can take the lead in building a concerted Whole-of-Government network that can act and respond flexibly in strengthening Singapore's cyber security. By being part of a strong cyber defence network that is better able to deal with cyber attacks, MAJ Xu believes that the SAF can then fulfil its mission of enhancing the peace and security of Singapore.

LTA Julie Lim Yee Sin's 'The Value of Sustainability for the SAF' is the second prize-winning essay. This essay explores the inherent link between sustainability and national security, and discusses what sustainability means for the SAF. According to LTA Lim, the SAF is instrumental to Singapore's development—not only in enhancing security, but also in contributing to the community. In the face of emerging security threats, SAF operations have evolved beyond a traditional defence role. By investing in resource sufficiency and impact management, the SAF can embrace the uncertainties of our complex security landscape and better position itself to protect Singapore's national interests. LTA Lin's concludes that achieving this, however, is no mean feat. Besides utilising technology as a tool to enhance sustainability, the SAF ultimately requires innovation and the collective effort of its people to drive any changes. If we see these processes through the eyes of sustainability and find the means to streamline them, via the strategies discussed or otherwise, the SAF is well underway to start enhancing sustainability and optimising performance. The value of sustainability for the SAF, and consequently, for Singapore, is priceless.

The third prize-winning essay entitled 'Maritime Terrorism Threat in Southeast Asia and its Challenges' is by ME6 Joses Yau Meng Wee. ME6 Yau highlights that the threat of terrorism is always present, but the public was only given a wake-up call to the devastating impacts of terrorism after the September 11 attacks in the US. Since then, many countries have stepped up their counter-terrorism efforts and measures. ME6 Yau examines the terrorism threat in Southeast Asia, exploring the possible scenarios of a maritime terrorist attack in the region and assesses the region's counter-terrorism efforts that have been put in place. He analyses the efforts of the Association of Southeast Asian Nations (ASEAN) in fighting terrorism and acknowledges that confidence-building measures, shared intelligence, capacity building and enhancing interoperability have been effective in deterring, detecting and disrupting maritime terrorism. ME6 Yau also introduces an Opportunity, Capability and Intent (OCI) framework as a useful way of doing threat assessments, to further anchor his argument that the terrorism threat in Southeast Asia remains a clear and present danger.

Besides presenting the top three prize-winning essays from the 2015/2016 CDFEC, we are also pleased to feature three essays whose topics range from the future of airpower to a design of multi-domain command and control information systems to social intelligence and motivation theories.

The essay, 'Unmanned Aerial Vehicles and the Future of Airpower: A Technological Perspective' is written by ME4 Gerald Goh Qi Wen. In this essay, ME4 Goh aims to give a technological perspective of the future of airpower, as well as a detailed analysis of unmanned aerial vehicles' (UAV) role in operations today and its potential advantages and disadvantages. According to ME4 Goh, since the invention of the aeroplane by the Wright Brothers in 1903, developments in aerial space, particularly in airpower, have moved at a rapid pace. For countries whose militaries have developed a competent air force, airpower gives them a myriad of capabilities to protect their country's air space and security, such as the ability of airpower to access targets beyond the capabilities of the army and navy and to effectively destroy key infrastructure or high value targets with its penetration and range. ME4 Goh concludes that UAVs will eventually take over manned platforms in the second half of this century when the technologies for Unmanned Combat Aerial Vehicles (UCAV), unmanned strategic bombers and even unmanned helicopters and tanker/transport are expected to mature. He further adds that this future is dependent on the willingness of military forces and political governments to expand the roles of UAVs which will in turn drive their research and development, leading to UAVs which will eventually match, and even surpass manned platforms in performance and efficiency.

ME5 Chua Zhongwang's essay on 'Framework for Identifying Requirements in the Design of Multi-Domain Command and Control Information System for Tri-Service Integration' examines the challenges in designing a Command and Control Information System (CCIS) that shortens the Observe-Orientate-Decide-Act cycle for an integrated Armed Force. This involves the co-ordination of air, land and sea assets of the Armed Forces, as well as cyber security necessary to ensure the robustness and resilience of the system. In this essay, ME5 Chua explores the mission-domains requirements of the CCIS and the impact of the environment and tactical operations at the different air-land-sea physical domains. He also proposes a framework in the Requirement Analysis to achieve comprehensive requirements for CCIS system design across multi-domain operations.

The essay, 'Social Intelligence and Motivation Theories in Transforming the RSAF' is written by CPT Varun Kumar Rai, LTA Benjamin Tong Yong Wei & LTA Dustin Jee Kam Chin. The authors highlight that the working culture in the Republic of Singapore Air Force (RSAF) started out as a hierarchy culture, like most militaries. However, given the recent technological advances and shifts towards a more integrated and interdependent military, there has been a notable shift towards a somewhat clan culture. This essay aims to explain the shift in culture and its potential merits. It also aims to critically view the place that social intelligence has in this new culture and the roles that different motivational theories may have on the individual. The authors also feel that an understanding of motivational theories will allow the RSAF to keep her people on the 'edge of their seat', maintaining a healthy balance between the two extremes of staying stagnant due to being unmotivated and complacent from too much motivation. The authors also feel that having a deep understanding of motivation will help build a cohesive and nurturing working environment for the RSAF.

The POINTER Editorial Team

FINDING SAF'S PLACE IN THE CYBER AGE

by **MAJ Sebestian Xu**

Abstract:

With cyber space being widely recognised as a fast-expanding domain of modern warfare, militaries around the world are faced with a threat that is very real. Attacks have increased in recent years, and countries such as Russia, the United States (US) and Iran have fallen victim to cyber attacks. Because of the nature of cyber attacks, the rules that generally govern modern warfare in domains such as land, air, sea and space will not apply in the cyber domain. In this essay, the author discusses the challenges that the Singapore Armed Forces (SAF) are faced with in today's cyber age, and highlights the steps it must take in order to ensure continued peace and security in Singapore.

Keywords: Cyberspace; Threat; Modern Warfare; Cyber Age; Cyber Domain

INTRODUCTION

There is growing recognition that cyberspace is a new and fast-expanding domain of modern warfare. In 2004, the United States (US) expressly recognised cyberspace as a separate domain of battlespace, beyond the traditional domains of air, land, sea and space.[1] In 2011, retired General Michael Hayden, former Director of the National Security Agency and Central Intelligence Agency, remarked that "like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, cyber."[2]

The novel and evolving nature of this domain of modern warfare poses new challenges to military forces around the world. The threat is real, as can be seen from the escalating frequency and scale of cyber attacks in recent years. In 2007, Russia was accused of launching cyber attacks on Estonia after the Baltic state removed a Soviet war memorial in central Tallinn. The attack affected the websites of the Estonian presidency and parliament as well as Estonian ministries, political parties, news, organisations and banks.[3] One year later, Russia was similarly accused of attacking the websites of Georgia's president, parliament, foreign ministry, news agencies and banks, inundating them with millions of requests—known as distributed denial of service (DDOS) attacks—and causing the websites to shut down.[4] In this instance, the cyber attacks were followed by Russia's physical invasion of Georgia. In 2010, the Stuxnet worm was discovered.[5] The worm, believed to have been jointly developed by the US and Israel, destroyed close to 1,000 of the 5,000 centrifuges at Iran's Natanz nuclear facility, sabotaging the country's nuclear enrichment programme.[6] Singapore has also been the target of cyber-attacks. In 2013, a hacker going by the name of 'The Messiah', and who claimed to be part of the Anonymous international hacker collective, hacked into a number of websites, including those of the People's Action Party Community Foundation, Ang Mo Kio Town Council, The Straits Times, Seletar Airport, the Prime Minister's Office (PMO) and the Istana.[7] Singapore's connectivity and the push to become a Smart Nation make the nation a prime target for cyber attacks.[8] It is thus imperative to examine Singapore's position vis-à-vis cyber security and, more importantly, the role of the Singapore Armed Forces (SAF) in this new cyber age.

It can be dangerous if the rhetoric of conventional warfare is loosely applied to cyber attacks, or more generally, cyber operations.

This essay argues that one of the greatest challenges the SAF faces in dealing with cyber war is that cyber attacks defy categorisation within the conventional rhetoric and theories of war. Consequently, it is difficult to apply customary international law to cyber attacks as cyber operations are unlikely to qualify as acts of war. The SAF must thus find a new niche for itself in defending Singapore in the cyber realm. In keeping with the multi-faceted nature of cyberspace and cyber warfare, the SAF must expand its role beyond the conventional understanding of military operations; more importantly, this new role will require greater integration with other ministries, government agencies and even the private sector, in order to achieve a nimble, wide-ranging approach to strengthening Singapore's cyber defence.

APPLYING THE RHETORIC OF WAR TO CYBER ACTIVITIES

It can be dangerous if the rhetoric of conventional warfare is loosely applied to cyber attacks, or more generally, cyber operations. The spectrum of cyber operations and activities can range from cyber vandalism to cyber crime, cyber espionage, cyber terrorism, cyber attacks and even cyber war. The mass media regularly uses the term 'cyber attacks' when reporting on malicious cyber activities, but when their scale and effects are considered, many of these activities fall below the threshold of an 'armed attack' as understood in international law.[9] Loosely applying rhetoric that uses such terminology conflates genuine cyber attacks with other activities like cyber crime. Maintaining the distinction between cyber attacks and other forms of cyber operations is important because they fall under different legal regimes and involve different rights and obligations while conferring different types of protection. In particular, applying the rhetoric of war too liberally could cause states to overstep legal boundaries and respond too aggressively and disproportionately. In the case of the cyber operations that targeted Singapore in 2013, one would more accurately term them as acts of cyber vandalism or cyber crime, but certainly not cyber attack or cyber war. Those operations resulted in the defacement of webpages and disruption of services, but can hardly be considered to have an impact equivalent to that of a kinetic attack on the affected institutions. The appropriate response should thus come from law enforcement, as was the case, rather than the military. It is thus important to be clear on when the SAF can and should be involved in any response to cyber attacks.

ARE CYBER ATTACKS ACTS OF WAR?

The mission of the SAF is '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.'[10] The words 'should these fail, to secure a swift and decisive victory over the aggressor' should be read in the context of war.[11] However, the question then arises of whether this aspect of the SAF's mission is applicable to cyber war—and more specifically, whether cyber attacks qualify as acts of war.

Those who argue that cyber attacks can never constitute acts of war often adopt the view that cyber attacks can cause only limited damage, mostly of an economic nature.[12] According to the principles of customary international law, economic coercion and pressure generally do not constitute an impermissible 'use of force'.[13] However, it is becoming increasingly evident that cyber attacks can cause physical damage beyond the economic sphere. Stuxnet is one clear example of how cyber attacks can cause considerable damage to infrastructure. In fact, the *Tallinn Manual* on the International Law Applicable to Cyber Warfare—a study of how extant international legal norms can be applied to cyber conflict and warfare, prepared by an independent International Group of Experts (IGE) at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence—presumes that Stuxnet constituted a 'use of force'.[14]

Law professor Larry May has another argument to support the view that cyber attacks do not constitute war. He cites the definition of war put forth by German jurist Samuel Pufendorf: a 'state of men who are naturally inflicting or repelling injuries or are striving to extort by force what is due to them.'[15] May argues that since cyber attacks are not aimed at inflicting injuries on people but rather on computers, they do not constitute war.[16]

On the other hand, in the *International Strategy for Cyberspac*e published by the White House in 2011, the US did not rule out the possibility of a military response to 'hostile acts in cyberspace', effectively making clear that the US accepts that cyber attacks can be considered acts of war.[17] It did not, however, establish the threshold beyond which a cyber attack would warrant a military response.[18]

The differing views on cyber-attacks as acts of war thus give rise to a quandary. It can be argued that a cyber operation rising to the level of an 'armed attack' should be considered an act of war; however, given the nature of cyber operations where targets and the damage caused are often less tangible, it is difficult to define when a cyber attack is equivalent to a hostile armed attack.[19] One often cited example is a massive cyber attack on a state economic infrastructure such as the stock exchange, resulting in the state's economy being crippled. Would such an operation qualify as an act of war? What international laws can be applied in this context?

A LOOK AT INTERNATIONAL LAW

In cyberspace, the concept of boundaries becomes nebulous. The corollary of this is that it becomes difficult to apply the moral and legal doctrines that were developed for the purpose of regulating sovereignty and physical boundaries.[20] Nevertheless, it is widely accepted that the international laws governing armed conflicts should be applicable to cyber operations. In the 2013 Report of the Group of Governmental Experts (GGE), a group set up by the United Nations (UN) General Assembly to examine threats in cyber space, it was stated that

The logo of NATO Cooperative Cyber Defence Centre of Excellence.

"international law, and in particular the Charter of the UN, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible Information and Communications Technologies (ICT) environment."[21] The IGE that produced the *Tallinn Manual* was also in agreement that both *jus ad bellum* (a body of international law determining when the use of force is justified) and *jus in bello* (another body of law governing how states should conduct themselves during periods of armed conflict) apply to cyber operations.[22] While there are other relevant sources of international law, most academic debate has centred on the application of these two bodies of law to cyber operations. This essay will not discuss *jus in bello*, which applies after it has already been established that the state is involved in an armed conflict. Instead, this essay concerns itself with *jus ad bellum*, particularly in the context of the SAF's relevance in cyber operations that are targeted at Singapore.

In cyberspace, the concept of boundaries becomes nebulous. The corollary of this is that it becomes difficult to apply the moral and legal doctrines that were developed for the purpose of regulating sovereignty and physical boundaries.

JUS AD BELLUM – RELEVANT PROVISIONS IN THE UNITED NATIONS CHARTER

The International Court of Justice (ICJ) has recognised that the restrictions on the use of force in the Charter of the UN correspond to the customary international law of *jus ad bellum*.[23] Article 2(4) of the Charter of the UN provides that 'all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.'[24] However, an exception to this can be found in Article 51, which states that 'nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.'[25]

It has been argued that for Article 2(4) to apply to cyber operations, there are three conditions to be met: (1) the cyber operation needs to be attributed to a state; (2) the cyber operation must amount to either a 'threat' or a 'use of force'; and (3) the threat or use of force must be exercised in the conduct of 'international relations'.[26]

The following discussion examines the challenges of applying the conditions of Article 2(4) to cyber operations. It assumes, however, that the third condition can be met, thus excluding examples that fall outside the scope of Article 2(4) such as the use of force by a state against non-state actors within its own territory.

THE PROBLEM OF ATTRIBUTION

It is clear that a central problem in cyber operations is attributing acts in cyber space to specific actors. One example is the use of botnets to perform DDOS attacks. When hijacked computers are used to launch such attacks, identifying the source of the attack becomes complicated. Coupled with the technological ability to obfuscate the source of cyber-attacks, attribution can sometimes be a near impossibility. In the case of the attacks on Estonia in 2007, analysts have still not been able to produce evidence of direct Russian involvement.[27] Similarly, while the US and Israel are widely suspected to be behind Stuxnet, the authors of the worm have not been officially identified.[28]

The waters are muddied even further in the case of a cyber attack fronted by a non-state actor. If a non-state actor, such as an individual hacker, criminal organisation, armed group, or even a patriotic hacker, carries out a cyber operation on his (its) own accord, it would then fall outside the scope of *jus ad bellum*. However, Article 8 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts states that 'the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.'[29] Hence, if it can be proven that such a relationship exists between a non-state actor in a cyber operation and a state, the cyber operation can be attributed to the state. However, the challenge of attribution is two-fold here: firstly, in attributing the cyber operation to the non-state actor; secondly, in establishing the connection between the non-state actor and the state, given that the non-state actor can always maintain plausible deniability.

THE PROBLEM OF THE 'USE OF FORCE'

There are several approaches to assessing whether a cyber operation qualifies as a 'use of force' prohibited under Article 2(4). The most widely-supported approach is based on the scale and effects of the action.[30] In the International Court of Justice (ICJ)'s judgment in *Nicaragua v. United States of America ("Nicaragua")*, the Court held that the 'scale and effects' are to be considered when determining if particular actions amount to an 'armed attack'.[31] Referencing this position, the IGE proposed Rule 11 of the *Tallinn Manual*: 'a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.'[32] This approach seeks to identify cyber operations with kinetic actions that the international community would describe as uses of force. The IGE also explicitly stated that 'acts that injure or kill persons or damage or destroy objects are unambiguously uses of force.'[33] In line with this reasoning, the IGE considered Stuxnet a use of force, given the damage it inflicted on the Natanz nuclear facility.

In the example of a cyber operation that incapacitates a stock exchange and cripples the target state's financial markets, it can be argued that the operation led to no injuries, death, or physical damage to any object, and hence the cyber operation should not constitute a 'use of force'. However, if the stock exchange were to be bombed kinetically, this would indisputably be considered a 'use of force'. In such an attack, the most severe consequence—indeed, the greatest intended effect of the attacker—would likely be the impact on the state's economy and the psychological effect of crippling a symbol of the state's prosperity, over and above the physical damage and injuries caused. The net scale and effect of the kinetic bombing can be said to be same as the cyber operation. Furthermore, the metaphorical scaling of walls that takes place when the culprit behind the cyber operation takes down the stock exchange's firewalls and cyber defences can have additional psychological effects on the population of a technologically advanced country: while a kinetic bombing can be physically avoided by evacuation or prevented pre-emptively, no one is safe from a cyber attack. In this light, it may be argued that the 'scale and effects' of a cyber operation can be comparable to a kinetic attack and thus should qualify as a 'use of force'.[34]

IS THERE A RIGHT TO SELF-DEFENCE IN CYBER OPERATIONS?

It has been demonstrated that there are numerous challenges that stand in the way in determining whether a cyber operation qualifies as a 'use of force' prohibited by Article 2(4). However, even if a cyber operation can be incontrovertibly attributed to a state and definitively shown to constitute a 'use of force', it may only constitute an unlawful action under Article 2(4) that does not necessarily warrant a military response.

Article 51, however, permits a state to exercise the right of self-defence and respond militarily to an 'armed attack'.[35] The question that must be considered is whether state military forces can invoke the right of self-defence in responding to cyber operations. For self-defence to be permissible, there must first be an 'armed attack' on the state. In its *Nicaragua* judgement, the ICJ recognised 'armed attack' as a subset of the 'use of force'.[36] While all 'armed attacks' are 'uses of force', the reverse does not hold true. The ICJ also noted that 'the most grave forms of the use of force' constitute an 'armed attack', and that whether a particular action constitutes an 'armed attack' would depend on its 'scale and effects'.[37] The IGE took note of this in proposing Rule 13 of the *Tallinn Manual*, in which it is stated that 'whether a cyber operation constitutes an armed attack depends on its scale and effects.'[38] However, the IGE was also of the view that the law was unclear as to the threshold for a cyber operation to qualify as an 'armed attack'.[39]

While Article 51 permits military response as an act of self-defence, it is once again debatable whether and when a cyber operation would rise to the level of an 'armed attack' that triggers this right. It is argued that while standalone cyber operations may possibly constitute 'uses of force', it is unlikely that they would rise to the level of 'armed attacks'. For this reason, it is unlikely that military forces can rely on the right of self-defence in responding to standalone cyber operations. Instead, this right would likely be triggered only when cyber operations are conducted alongside traditional kinetic military operations.[40]

THE ROLE OF THE MILITARY IN CYBER-ATTACKS

Given the difficulties that military forces face in determining whether they can and should respond to cyber attacks, the question then is how the SAF can fulfil its mission to enhance Singapore's peace and security in the face of increasing cyber threats to the nation.

MINDEF

The new Defence Cyber Organisation (DCO) will strengthen the SAF's cyber defence in a cyber attack.

The central tension that the SAF faces is whether it should play both offensive and defensive roles in cyber operations. Other military forces have opted to take on clearly offensive roles. The US Cyber Command and Israel's Military Intelligence Unit 8200 are military outfits that boast cyber offensive capabilities. The People's Liberation Army has set up a central cyber warfare command, which has been said to be "an official sign that cyber-attacks would be used in a military conflict."[41]

However, it is argued that it would be ill-advised for the SAF to pursue cyber offensive capabilities as it would go against the grain of Singapore's defence policy, which is built upon the two pillars of deterrence and diplomacy.[42] While it can be argued that having strong cyber offensive capabilities would strengthen the deterrence factor, it could be counter-productive for diplomacy. Furthermore, the use of cyber attacks as a military response to an armed attack falls under the regime of *jus in bello*. There are even more difficulties in applying this body of international law to cyber operations, such as the problems of distinction (for instance, whether civilian hackers behind cyber attacks are considered combatants and can be lawfully targeted) and proportionality (for instance, the appropriate response to a cyber operation that does not result in collateral civilian death, injury, damage or destruction).[43]

Given that it will be challenging to determine whether cyber operations that are carried out against Singapore justify a military response, and in particular a response in the form of counter-cyber operations, the SAF should focus on the defence of Singapore's networks and systems. As the nation becomes increasingly connected, this will require greater integration with other ministries, government agencies and even the private sector.

A WHOLE-OF-GOVERNMENT APPROACH TO CYBER DEFENCE

The Cyber Security Agency (CSA) of Singapore is a national body set up in April 2015 to oversee cyber security strategy, education, outreach, and industry development.[44] It co-ordinates public and private sector efforts to protect national systems from cyber threats, including in the energy, water and banking sectors.[45] The national defence systems do not come under the CSA's umbrella of responsibilities but remain under the SAF's purview.

However, one point to consider is whether the segregation of responsibilities in cyber defence between the SAF and government agencies like the CSA should still be maintained going forward. There are several reasons why maintaining the segregation can become increasingly artificial. Firstly, as the discussion above on the shifting, expansive nature of cyber operations shows, tackling the threat of cyber-attacks requires moving beyond the conventional thinking about warfare. The definitions of national security and national defence in the cyber sphere may have to be expanded beyond the purely military to include other sectors of activities that are crucial to the state such as the economy and water resources. Hence, a more flexible and cohesive approach shared by the SAF and other agencies involved in cyber security would help the nation as a whole in enhancing cyber defence.

Secondly, segregating responsibilities between the SAF and other agencies may not be practical given the need for shared expertise and manpower in cyber security. Given that the cutting edge of online technology is likely to be found in the private sector, it makes sense to extend co-operation and interaction across the people-private-public sectors, to allow for greater cross-pollination of ideas and knowhow.

A Whole-of-Government approach would also call for deeper inter-ministry co-operation. Programming classes have been introduced in schools by the Ministry of Education (MOE) and the Infocomm Development Authority (IDA) of Singapore since 2014. The SAF, as well as the CSA, can leverage on this effort to grow a pool of cyber security specialists for the nation.

Furthermore, encouraging greater co-operation among agencies involved in cyber security is in line with the push in the public service to co-ordinate and 'join the dots' across ministries and agencies, as can be seen from the creation of co-ordinating agencies such as the Prime Minister's Office Strategy Group and the Municipal Services Office, and the increase in the number of Co-ordinating Ministers that straddle various portfolios. Besides reducing the risk of operating in silos, co-ordination also enriches the vocabulary and problem-solving skills of individual agencies because 'different agencies can often use different vocabulary and perceive the world rather differently.'[46] In the context of cyber security, the SAF's ability to defend Singapore against cyber threats would only be enriched if it can draw on the vocabulary and expertise of other groups and agencies that approach cyber operations from different perspectives.

Mr Chan Yeng Kit, Permanent Secretary (Defence), speaking about the importance of cybersecurity at the 2016 Cyber Defender Discovery Camp.

The SAF already has strong partnerships with the Defence Science Organisation (DSO), the Defence Science and Technology Agency (DSTA) and other local defence industry partners such as Singapore Technologies (ST) Engineering.[47] The CSA could be brought in as another such partner. In addition, the SAF could move beyond simply enlisting the services of these partners to possibly cross-deploying personnel. Such an arrangement would strengthen mutual understanding and facilitate the exchange of knowledge, which could lead to the discovery of new ways to strengthen existing cyber security measures. This would also help the SAF develop in-house expertise in cyber defence and hone its cyber defence capabilities. However, due consideration will have to be given to the information that such personnel can access so as not to compromise security.

A Whole-of-Government approach would also call for deeper inter-ministry co-operation. Programming classes have been introduced in schools by the Ministry of Education (MOE) and the Infocomm Development Authority (IDA) of Singapore since 2014.[48] The SAF, as well as the CSA, can leverage on this effort to grow a pool of cyber security specialists for the nation. One suggestion would be for the SAF and CSA to work with the MOE to offer joint scholarships to students who excel in and have a keen interest in cyber security. Scholarship holders would have the opportunity to pursue a career in cyber security with either organisation, or perhaps be rotated through both organisations. Stints with private sector technology groups and companies could also be arranged. Both the SAF and the CSA would ultimately benefit from such an arrangement as they can increasingly draw from a pool of professionals who can contribute to strengthening the nation's cyber-defence.

CONCLUSION

The new domain of cyber operations sits uncomfortably with conventional doctrines on war and the tenets of international law. Consequently, the rules that apply in this cyber age are difficult to define. Even though it is hard to determine whether and when the SAF can be called upon to respond to standalone cyber operations against Singapore, it still has an essential role to play in cyber defence. The SAF must understand that it is playing by different rules in the cyber domain; hence, its role cannot be restricted to leading independent, purely military, efforts. As Singapore becomes increasingly connected and cyber operations become increasingly sophisticated, the SAF could take the lead in building a concerted, Whole-of-Government network that can act and respond flexibly in strengthening Singapore's cyber security. By being part of a strong cyber-defence network that will deter potential cyber-attacks, the SAF can then fulfil its mission of enhancing the peace and security of Singapore.

BIBLIOGRAPHY

Blank, Laurie R, "Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace." In Cyberwar: Law and Ethics for Virtual Conflicts, edited by Jens David Ohlin, Kevin Govern and Claire Finkelstein, 76-101. Oxford: Oxford University Press, 2015.

"Central cyber warfare command for PLA," The Straits Times, 2014.

http://www.straitstimes.com/asia/east-asia/central-cyber-warfare-command-for-pla.

"Charter of the United Nations: Chapter I," United Nations. 2016.

http://www.un.org/en/sections/un-charter/chapter-i/index.html.

"Charter of the United Nations: Chapter VII," United Nations. 2016.

http://www.un.org/en/sections/un-charter/chapter-vii/index.html.

"Defence Policy and Diplomacy," Ministry of Defence, Singapore. 2016.

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

Finkelstein, Claire and Kevin Govern, introduction to Cyberwar: Law and Ethics for Virtual Conflicts, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein, ix-xx. Oxford: Oxford University Press, 2015.

Focarelli, Carlo, "Self-defence in cyberspace," in Research Handbook on International Law and Cyberspace, ed. Nikolaos K. Tsagourias and Russell Buchan, 255-283. Cheltenham: Edward Elgar Publishing Ltd, 2015.

Gill, Terry D. "International humanitarian law applied to cyber-warfare: Precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict," in Research Handbook on International Law and Cyberspace, ed. Nikolaos K. Tsagourias and Russell Buchan, 366-379. Cheltenham: Edward Elgar Publishing Ltd, 2015.

Hayden, Michael V. "The Future of Things 'Cyber'," Strategic Studies Quarterly 5 (2011): 3-7.

Hio, Lester, "Coding and programming classes for students to smooth transition to Smart Nation," The Straits Times, 2015.

http://www.straitstimes.com/singapore/education/coding-and-programming-classes-for-students-to-smooth-transition-to-smart-nation.

International Court of Justice, "Case Concerning the Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits),"Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 1986. http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5.

International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts." In Report of the International Law Commission on the work of its fifty-third session, (2008), 30-143.

http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

Katz, Yaakov, "Military reveals for first time that it uses cyber space to gather intelligence, conduct military operations," The Jerusalem Post, 2012.

http://www.jpost.com/Defense/IDF-admits-to-using-cyber-space-to-attack-enemies.

Kushner, David, "The Real Story of Stuxnet," IEEE Spectrum, 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Markoff, John, "Before the Gunfire, Cyberattacks," The New York Times, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html.

May, Larry, "The Nature of War and the Idea of 'Cyberwar'," in Cyberwar: Law and Ethics for Virtual Conflicts, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein, 3-15. Oxford: Oxford University Press, 2015.

Myers, Richard B. Chairman of the Joint Chiefs of Staff, "The National Military Strategy of the United States of America," 2004.

Ong, Hong Tat, "Forging a technological edge," Cyber Pioneer, 2010. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2010/mar10_fs2.html.

"Our Organisation," Cyber Security Agency Singapore, 2015. https://www.csa.gov.sg/about-us/our-organisation.

Roscini, Marco, "Cyber operations as a use of force," in Research Handbook on International Law and Cyberspace, ed. Nikolaos K. Tsagourias and Russell Buchan, 233-254. Cheltenham: Edward Elgar Publishing Ltd, 2015.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran," The New York Times, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.

Sanger, David E and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," The New York Times, 2011. http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=0.

Schmitt, Michael N, foreword to Cyberwar: Law and Ethics for Virtual Conflicts, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein, v-viii. Oxford: Oxford University Press, 2015.

Schmitt, Michael N, Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," Berkeley Journal of International Law 27, n._ 1 (2009): 192-251.

"Speech by Mr Peter Ong, Head, Civil Service at the Public Service Leadership Dinner on 27 October 2015, at Orchard Hotel," Public Service Division. 2016. http://www.psd.gov.sg/media/speeches/speech-by-mr-peter-ong--head--civil-service--at-the-public-service-leadership-dinner

"Tallinn Manual," NATO Cooperative Cyber Defence Centre of Excellence. 2016. https://ccdcoe.org/research.html.

Tegos, Michael, "IDA wants to make Singapore a Smart Nation. Here's what you need to know," Tech in Asia, 2015. https://www.techinasia.com/singapore-smart-nation-2015.

Teng, Amelia, "More kids to learn programming in Smart Nation push," Asiaone, 2014. http://news.asiaone.com/news/singapore/more-kids-learn-programming-smart-nation-push.

Teo, Mavis, "Lessons Learnt from the Cyber Attacks," Challenge Online, 2014. http://www.challenge.gov.sg/print/feature/after-the-cyber-attacks.

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/singapore/new-cyber-security-agency-to-be-set-up-in-april-yaacob-ibrahim-to-be-minister-in-charge-of.

Traynor, Ian, "Russia accused of unleashing cyberwar to disable Estonia," The Guardian, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 2013. UN Doc A/68/98 8.

Wenworth, Travis, "How Russia May Have Attacked Georgia's Internet," Newsweek, 2008. http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

White House, "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," 2011.

Yoo, Christopher S, "Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures," in Cyberwar: Law and Ethics for Virtual Conflicts, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein, 175-194. (Oxford University Press, 2015).

ENDNOTES

1. Richard B. Myers, Chairman of the Joint Chiefs of Staff, "The National Military Strategy of the United States of America," (2004), 18.

2. Michael V Hayden, "The Future of Things 'Cyber'," Strategic Studies Quarterly 5 (2011): 4.

3. Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," The Guardian, May 17, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

4. Travis Wenworth, "How Russia May Have Attacked Georgia's Internet," *Newsweek*, 2008, http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

   John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

5. David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

6. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.

7. Mavis Teo, "Lessons Learnt from the Cyber Attacks," *Challenge Online*, 2014, http://www.challenge.gov.sg/print/feature/after-the-cyber-attacks.

8. Michael Tegos, "IDA wants to make Singapore a Smart Nation. Here's what you need to know," *Tech in Asia,* 2015, https://www.techinasia.com/singapore-smart-nation-2015.

9. Laurie R Blank, "Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace," in *Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein (*Oxford: Oxford University Press*, 2015), 78.

10. *MINDEF*. SAF MISSION. https://www.mindef.gov.sg/imindef/about_us/mission.html.

11. Ibid.

12. Claire Finkelstein and Kevin Govern, *introduction to Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein (*Oxford: Oxford University Press*, 2015), xv.

13. Laurie R Blank, "Cyberwar versus Cyber Attack," 78-79.

14. "Tallinn Manual," *NATO Cooperative Cyber Defence Centre of Excellence*, 2016, https://ccdcoe.org/research.html.

15. Larry May, "The Nature of War and the Idea of 'Cyberwar'," in *Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein (*Oxford: Oxford University Press*, 2015), 6.

16. Ibid., 6.

17. White House, "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," (2011), 14.

18. David E Sanger and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *The New York Times*, 2011, http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=0.

19. Michael N Schmitt, foreword to *Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein (Oxford: Oxford University Press, 2015), vi.

20. Claire Finkelstein and Kevin Govern, *introduction to Cyberwar: Law and Ethics for Virtual Conflicts*, xvi.

21. UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," (2013), UN Doc A/68/98 8.

22. Michael N Schmitt, foreword to *Cyberwar: Law and Ethics for Virtual Conflicts*, v.

23. Christopher S Yoo, "Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures," in *Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern and Claire Finkelstein (*Oxford: Oxford University Press*, 2015), 177.

24. "Charter of the United Nations: Chapter I," *United Nations*, 2016, http://www.un.org/en/sections/un-charter/chapter-i/index.html.

25. "Charter of the United Nations: Chapter VII," *United Nations*, 2016, http://www.un.org/en/sections/un-charter/chapter-vii/index.html.

26. Marco Roscini, "Cyber operations as a use of force," in *Research Handbook on International Law and Cyberspace*, ed. Nikolaos K. Tsagourias and Russell Buchan (Cheltenham: Edward Elgar Publishing Ltd, 2015), 234.

27. Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," Berkeley Journal of International Law 27, n._ 1 (2009): 208.

28. David Kushner, "The Real Story of Stuxnet."

29. International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts," in Report of the International Law Commission on the work of its fifty-third session, (2008), 47-49, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

30. Marco Roscini, "Cyber operations as a use of force," 236.

31. International Court of Justice, "Case Concerning the Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits),"Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 1986, para 195, http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5.

32. Michael N Schmitt, *Tallinn Manual*, 45.

33. Michael N Schmitt, *Tallinn Manual*, 48.

34. Marco Roscini, "Cyber operations as a use of force," 249.

35. Carlo Focarelli, "Self-defence in cyberspace," in *Research Handbook on International Law and Cyberspace*, 255.

36. International Court of Justice, "Nicaragua v. United States of America," para 191, 210.

37. Ibid, para 191.

Ibid, para 195.

38. Michael N Schmitt, *Tallinn Manual*, 54.

39. Michael N Schmitt, *Tallinn Manual*, 55-56.

40. Terry D. Gill, "International humanitarian law applied to cyber-warfare: Precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict," in *Research Handbook on International Law and Cyberspace*, 367.

41. Yaakov Katz, "Military reveals for first time that it uses cyber space to gather intelligence, conduct military operations," *The Jerusalem Post*, 2012, http://www.jpost.com/Defense/IDF-admits-to-using-cyber-space-to-attack-enemies.

"Central cyber warfare command for PLA," *The Straits Times*, 2014, http://www.straitstimes.com/asia/east-asia/central-cyber-warfare-command-for-pla.

42. "Defence Policy and Diplomacy," Ministry of Defence, Singapore, 2016, http://www.mindef.gov.sg/imindef/key_topics/defence_policy.html.

43. Terry D. Gill, "International humanitarian law applied to cyber-warfare," 375.

44. "Our Organisation," *Cyber Security Agency Singapore*, 2015, https://www.csa.gov.sg/about-us/our-organisation.

45. Irene Tham, "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/singapore/new-cyber-security-agency-to-be-set-up-in-april-yaacob-ibrahim-to-be-minister-in-charge-of.

46. "Speech by Mr Peter Ong, Head, Civil Service at the Public Service Leadership Dinner on 27 October 2015, at Orchard Hotel," *Public Service Division*, 2016, http://www.psd.gov.sg/media/speeches/speech-by-mr-peter-ong--head--civil-service--at-the-public-service-leadership-dinner

47. Hong Tat, Ong, "Forging a technological edge," *Cyber Pioneer*, 2010, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2010/mar10_fs2.html.

48. Amelia Teng, "More kids to learn programming in Smart Nation push," *Asiaone*, 2014, http://news.asiaone.com/news/singapore/more-kids-learn-programming-smart-nation-push.

Lester Hio, "Coding and programming classes for students to smooth transition to Smart Nation," *The Straits Times*, 2015, http://www.straitstimes.com/singapore/education/coding-and-programming-classes-for-students-to-smooth-transition-to-smart-nation.

MAJ Sebestian Xu is an AWO (C3) by vocation. He is currently a staff officer in the C4 Development Branch in C4 Group, Air Operations Department, and was previously from 203 SQN, Air Defence and Operations Command. MAJ Sebestian was a recipient of the Academic Training Award (Local) and holds a Bachelor of Engineering (Computer Engineering) (2nd Class Honours, Upper Division) from the National University of Singapore.

THE VALUE OF SUSTAINABILITY FOR THE SINGAPORE ARMED FORCES

by **LTA Julie Lim Yee Sin**

Abstract:

In the military sphere, sustainability is often overlooked or disregarded as being irrelevant. It may be seen to be in direct conflict with other objectives. Furthermore, sustainability measures may be ignored for the sake of convenience. The main concern of the Singapore Armed Forces (SAF) will always be of security, and safeguarding national interests. However, the SAF does plan for long-term measures to reduce inefficiency. This is especially prudent considering the large share of the national budget allocated to defence expenditure. This essay will attempt to address the roles that sustainability plays in the SAF as well as envision certain areas where measures to improve sustainability may be implemented.

Keywords: Sustainability; National Security; Social; Economic; Environmental; Technology; Energy

INTRODUCTION

The essence of sustainability is simple—'development that meets the needs of the present without compromising the needs of future generations to meet their own needs.'[1] However, it is far from trivial in its implementation, particularly when embedded within the complex task of planning for the future. Sustainability principles may be in conflict with other objectives, or simply disregarded for expediency. This essay explores the inherent link between sustainability and national security, and discusses what sustainability means for the SAF.

THE CONCEPT OF SUSTAINABILITY

Often associated with idealistic aims of 'eradicating poverty' or 'preventing global warming', sustainability has become an easily dismissed topic. However, the principles of sustainability encompass much more—defining an approach to balance competing objectives within certain limitations, rather than necessarily eliminating the issues mentioned.[2] Fundamentally, sustainability seeks to protect human life, and going a step further, to enhance the quality of life.[3] There are many sustainability frameworks adopted by various governments, organisations and even militaries.[4] These generally focus on the integration of three key dimensions—social, economic and environmental.[5] Social sustainability focuses on human capital and promotes social stability; economic sustainability optimises the management of finances; and environmental sustainability seeks to maintain the natural resources necessary for human life.

RELEVANCE TO NATIONAL SECURITY

The apparent duality between sustainability and national security is actually an intertwined relationship of mutual dependence, as depicted in *Figure 1*.

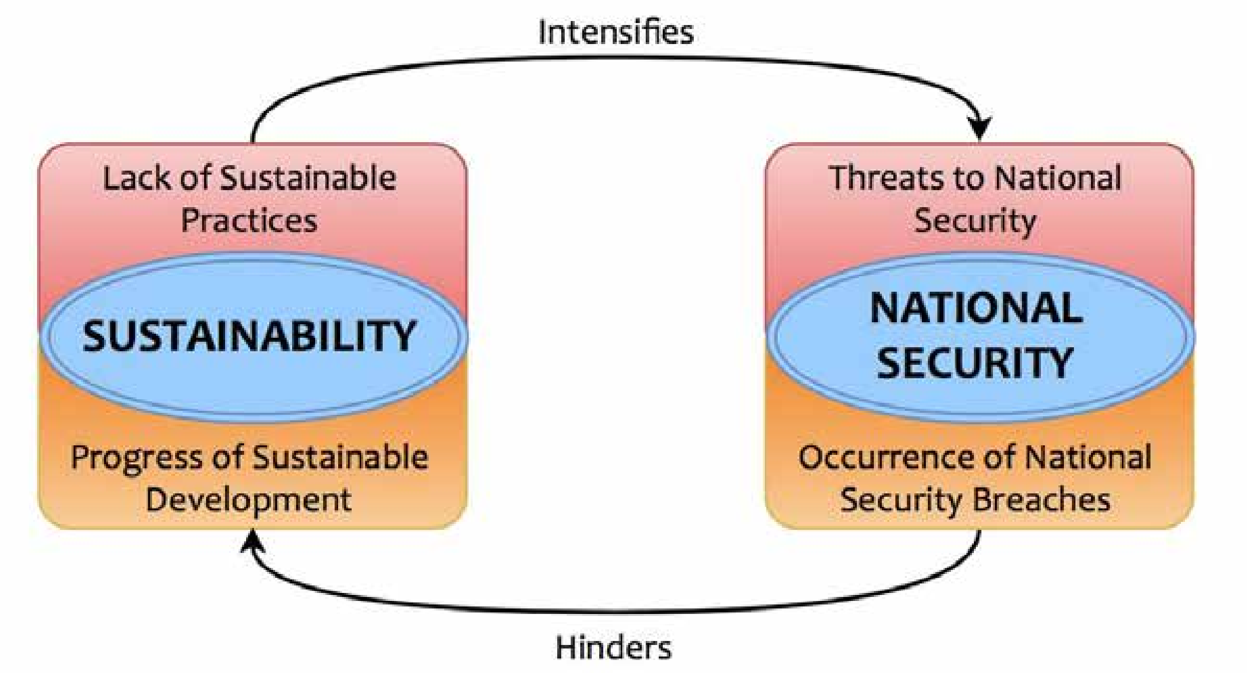

Intensifies
Lack of Sustainable Practices
SUSTAINABILITY
Progress of Sustainable Development
Threats to National Security
NATIONAL SECURITY
Occurrence of National Security Breaches
Hinders

Figure 1: Mutual Dependence of Sustainability and National Security

IMPLICATIONS OF NATIONAL SECURITY

The scope of national security has been broadened over the years, extending beyond the traditional state-centric notions of sovereignty and military security. In his 2016 addendum to the President's Address, Deputy Prime Minister and Co-ordinating Minister for National Security Mr Teo Chee Hean mentioned "a terrorist attack, a virus whether medical or cyber, food contamination, and social fissures," as examples of Singapore's "increasing challenging threat landscape."[6] Such issues may threaten Singapore's development in terms of social well-being, economic growth, and sustenance of critical infrastructures like energy, water and transport. The occurrence of national security breaches will thus hinder sustainable development.

IMPLICATIONS FOR NATIONAL SECURITY

Conversely, the lack of sustainable practices in turn intensifies threats to national security. This is a complex and vast issue, arising across the various domains, with implications on the global, regional and national scale. The environmental domain will be discussed here, as it represents the most evident form of sustainability, yet has the least intuitive implications for national security. The effects of unsustainable practices (such as burning of fossil fuels, deforestation and emission of greenhouse gases) on global warming and, in a broader context, on climate change have been extensively advocated against.[7] However, the impact that these issues have on national security is less frequently communicated.

Unlike other forms of security threats, environmental concerns are often overlooked because they are viewed as issues gradually occurring in the background, rather than immediate, imminent threats. The argument primarily rests on the premise that degradation of natural resources and vital life-support systems has extensive effects, such as mass migration, growth of terrorism and escalation of conflicts over resources.[8] Instead of analysing the multitude of consequences, a selection of consequences relevant in Singapore's context will be presented, though these examples are by no means exhaustive.[9]

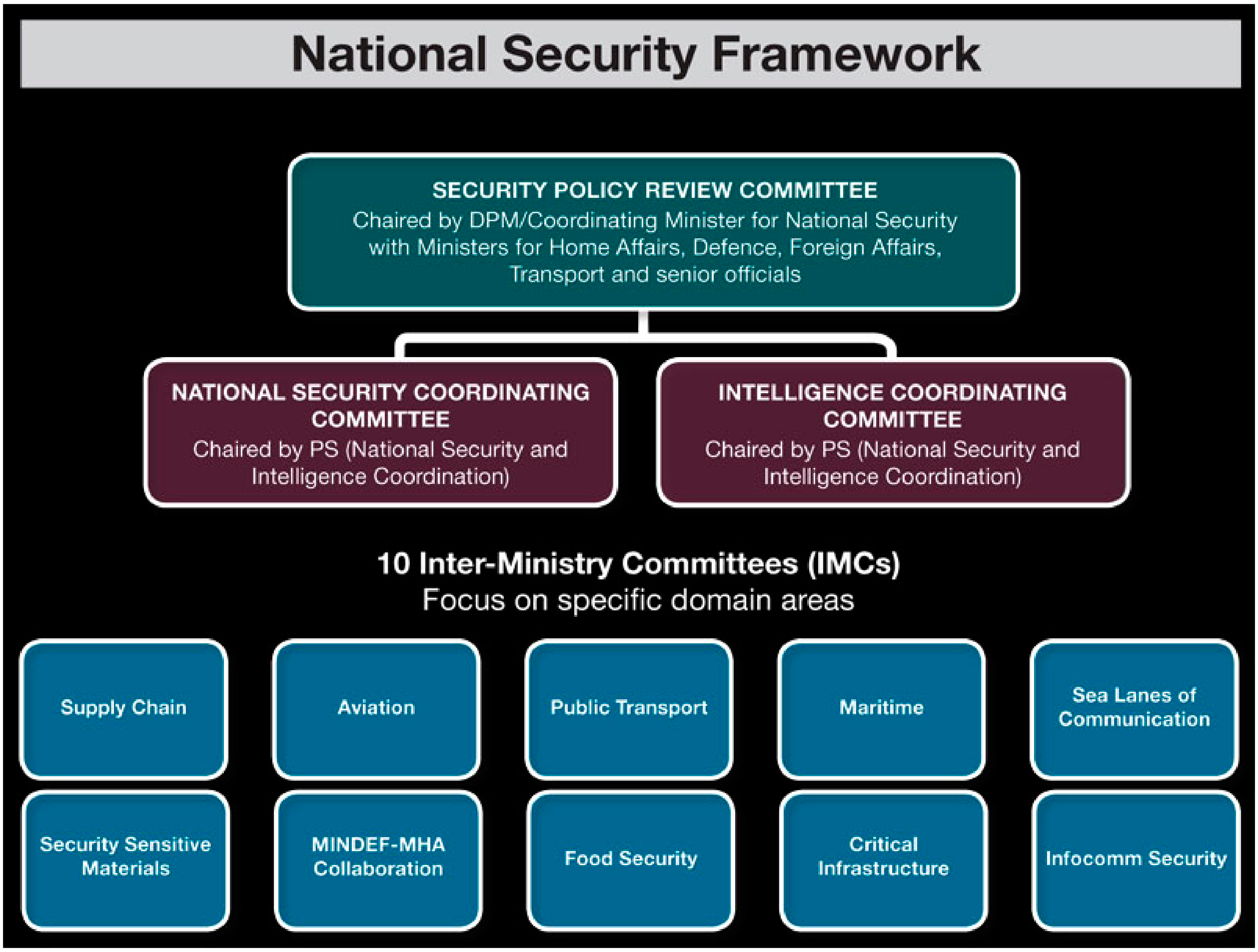
First, consider the direct impact of climate change. While global warming refers to the rise in the Earth's surface temperature, climate change extends to the effects of that, such as the rise in sea levels and extreme weather patterns like heavier rainfalls and droughts.[10] This could lead to prolonged dry spells that threaten Singapore's water supply, as reflected in the decline of reservoir water levels.[11] Though this may not be a cause for alarm since Singapore has invested significant efforts in ensuring sufficiency in our water supply, climate change does intensify vulnerabilities in water security on the national level.[12] As such, Singapore has certainly begun to acknowledge the growing threats and stay on top of them, even if they seem distant. For instance, in 2013, Singapore gained permanent observer status in the Arctic Council as developments there, such as the melting of the ice cap and the opening of new sea routes, will have "implications for Singapore as a low-lying island and international seaport."[13] Moreover, beyond the risks that seem to be waiting to happen, some consequences of climate change are already affecting the daily lives of Singaporeans.[14] For instance, warmer and wetter conditions have encouraged the spread of infectious diseases.[15] These include vector-borne diseases such as dengue fever and more recently, the Zika virus.[16]

Although these may seem to deviate from the traditional security definition, they still remain key considerations for Singapore's national interests, by threatening our water needs, economic position and in extreme cases, our existence.[17] Just as the scope of national security has been broadened to include growing threats like terrorism and cyber-attacks, climate change or, more generally, sustainability issues also pose a cause for concern. In some ways, the emergence of non-traditional security threats may even be a result of failures in sustainable development.

Arguably, Singapore as a 'tiny red dot' on the world map may not substantially contribute to resolving a global issue like climate change. Nevertheless, it should be recognised that at the regional level, unsustainable practices do lead to security issues as well. An example is the transnational haze crisis, which has become a human and national security threat from the health and socio-economic risks associated with its severity.[18] This even has a direct impact for the SAF, as outdoor activities and training have to be adjusted to ensure the health and safety of SAF service personnel.[19] To combat the pollution that has lasting health impacts for our population, and for our neighbours, the SAF also plays a part as a responsible member of the regional community. In 2015, the SAF deployed a Chinook helicopter, along with a Singapore Civil Defence Force team, to assist with firefighting operations in the Indonesian forests.[20] Unfortunately, this was a retrospective attempt to reduce the damage rather than to prevent it from happening, as it is difficult to curb illegal slash-and-burn practices.[21] Such issues are multi-faceted and not easily resolved, complicated by their transnational nature.

APPROACH TO NATIONAL SECURITY

In order to tackle these complex and evolving threats, it is thus important to 'anticipate rather than react'.[22] This may be conducted in the form of risk analyses, but can also be done by strengthening resilience. Strategies capitalising on the idea that 'prevention is better than cure' are intrinsically linked to the concept of sustainability. By ensuring sustainability in the first place, national interests are still pursued but less 'firefighting' is required as the focus is shifted away from threats and military



National Security Framework

SECURITY POLICY REVIEW COMMITTEE
Chaired by DPM/Coordinating Minister for National Security with Ministers for Home Affairs, Defence, Foreign Affairs, Transport and senior officials

NATIONAL SECURITY COORDINATING COMMITTEE
Chaired by PS (National Security and Intelligence Coordination)

INTELLIGENCE COORDINATING COMMITTEE
Chaired by PS (National Security and Intelligence Coordination)

10 Inter-Ministry Committees (IMCs)
Focus on specific domain areas

Supply Chain | Aviation | Public Transport | Maritime | Sea Lanes of Communication

Security Sensitive Materials | MINDEF-MHA Collaboration | Food Security | Critical Infrastructure | Infocomm Security

Figure 2: Singapore's National Security Framework

force.[23] This idea is captured in a 2011 paper titled ‘A National Strategic Narrative’, which highlights that "security means more than defence, and sustaining security requires adaptation and evolution, the leverage of converging interests and interdependencies."[24]

SINGAPORE’S FRAMEWORK

Although the military is often viewed as the primary agent of security, the idea that it cannot stand alone is not a new one. A 1987 United Nations (UN) Report aptly identified that "there are no military solutions to environmental insecurity."[25] Non-traditional security threats are typically multi-dimensional and transcend state boundaries. Hence, Singapore adopts a ‘whole-of-government’ approach to manage national security, shown in *Figure 2*. This allows the wide variety of traditional and non-traditional security threats to be comprehensively dealt with by the most appropriate specialist organisations. For instance, the sustainable development issues related to carbon emissions, water conservation or waste generation would fall under the purview of the Ministry of the Environment and Water Resources.[26]

At this point, it is worth distinguishing between two levels of sustainability—the sustainability of Singapore’s development in contrast with that of SAF operations. The former is on a larger, national scale, and contributed to by many government ministries. Collaboration with other agencies is necessary for a

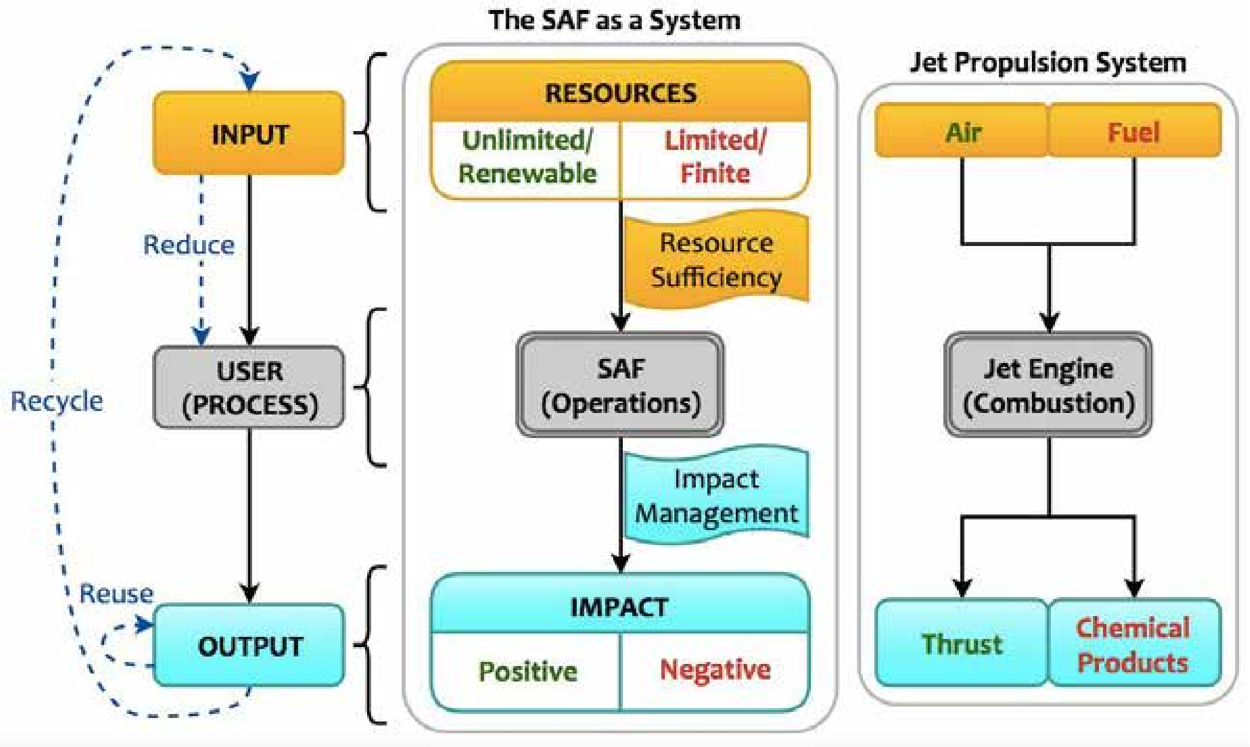


Figure 3: The SAF as a System of Inputs and Outputs

holistic approach, but the SAF still plays a key role as a driver for the rest of the Singapore community. Focus of the remaining discussion will be on the latter, to explore the possible value of sustainability within the SAF. This proposes sustainability principles as a means for the SAF to embrace the uncertainties of growing non-traditional security threats, by increasing our resilience to potential threats. This will contribute to, rather than deviate from, achieving our mission of enhancing Singapore's peace and security.

UNDERSTANDING SUSTAINABILITY FOR THE SAF

A simple model can be used to distil what sustainability means for the SAF, as illustrated in *Figure 3*. Just like a jet propulsion engine that utilises air and fuel for combustion to produce thrust and chemical products, the SAF is at the core of a system with inputs and outputs—as the user of a variety of resources to conduct operations, some impact will be generated alongside mission success. Some of these inputs may be 'unlimited' (air), and others finite in quantity (fuel). Similarly, some of these outputs may be positive (thrust), while others less so (greenhouse gases in the chemical products).

Just like a jet propulsion engine that utilises air and fuel for combustion to produce thrust and chemical products, the SAF is at the core of a system with inputs and outputs—as the user of a variety of resources to conduct operations, some impact will be generated alongside mission success.

Attaining sustainability in this model, therefore, requires that the process can go on forever, either with an infinite source at the input, or a loop from the output back to the input. This is in line with the '3Rs' concept that many will be familiar with: reduce the amount of input needed, reuse the product and recycle the output.[27]

PRINCIPLES OF SUSTAINABILITY

Focusing on the SAF in *Figure 3*, two key areas can hence be identified to ensure sustainability, namely resource sufficiency for the inputs and impact management of the outputs. The former seeks to balance the consumption and production of resources, while the latter attempts to reduce the overall footprint of activities. In order to achieve this, possible guiding principles for the SAF are listed in *Figure 4*.

Strategies targeting resource sufficiency are likely to have direct positive implications for the SAF, as these resources are necessary for operations. Conversely, strategies for impact management will affect the SAF indirectly, as the out-going arrow may consequently feed back into the system. For instance, utilising alternative energies (diversifying sources) will directly benefit the SAF in the face of depleting oil reserves, by providing flexibility in operations and reducing the logistics tail, while minimising carbon emissions (alleviating adverse effects) would have an indirect impact through climate change and national security considerations.[28]

Sustainability should also be studied in the various dimensions. When analysing what the social, economic and environmental dimensions represent for the SAF, it is appropriate to highlight that some aspects of sustainability have already been implicitly accounted for. As opposed to suggesting that the SAF may be lacking in sustainability, this essay proposes sustainability as a fresh lens through which the long-term enhancement of security and operations can be viewed.

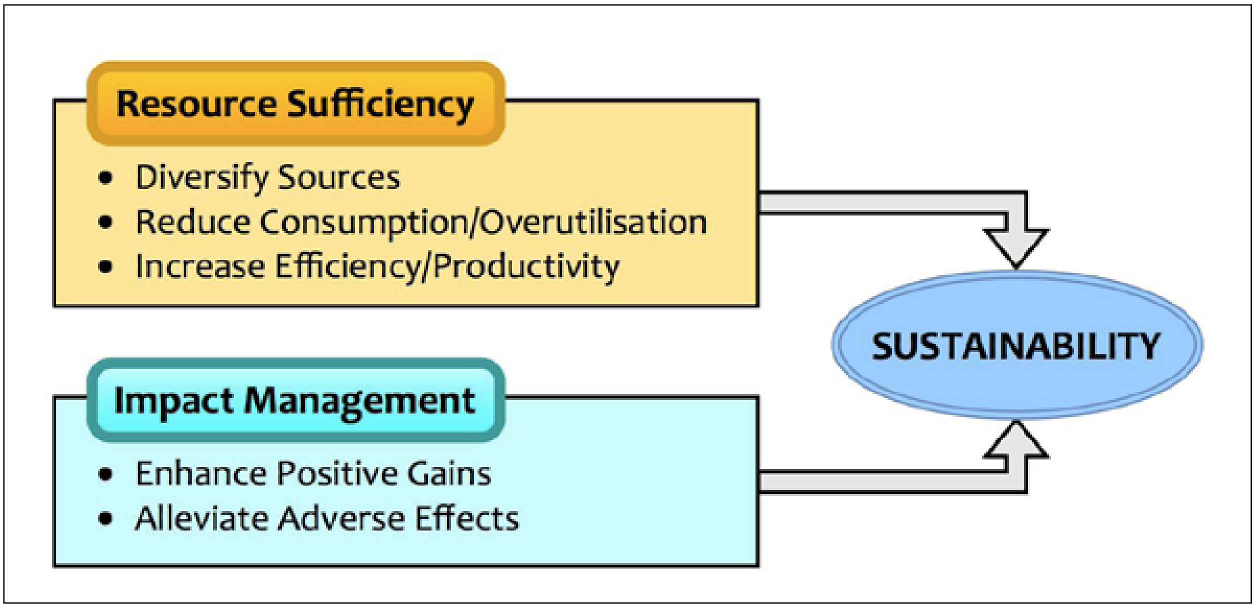

Resource Sufficiency
• Diversify Sources
• Reduce Consumption/Overutilisation
• Increase Efficiency/Productivity
Impact Management
• Enhance Positive Gains
• Alleviate Adverse Effects
SUSTAINABILITY

Figure 4: Guiding Principles for Resource Sufficiency and Impact Management

SOCIAL SUSTAINABILITY

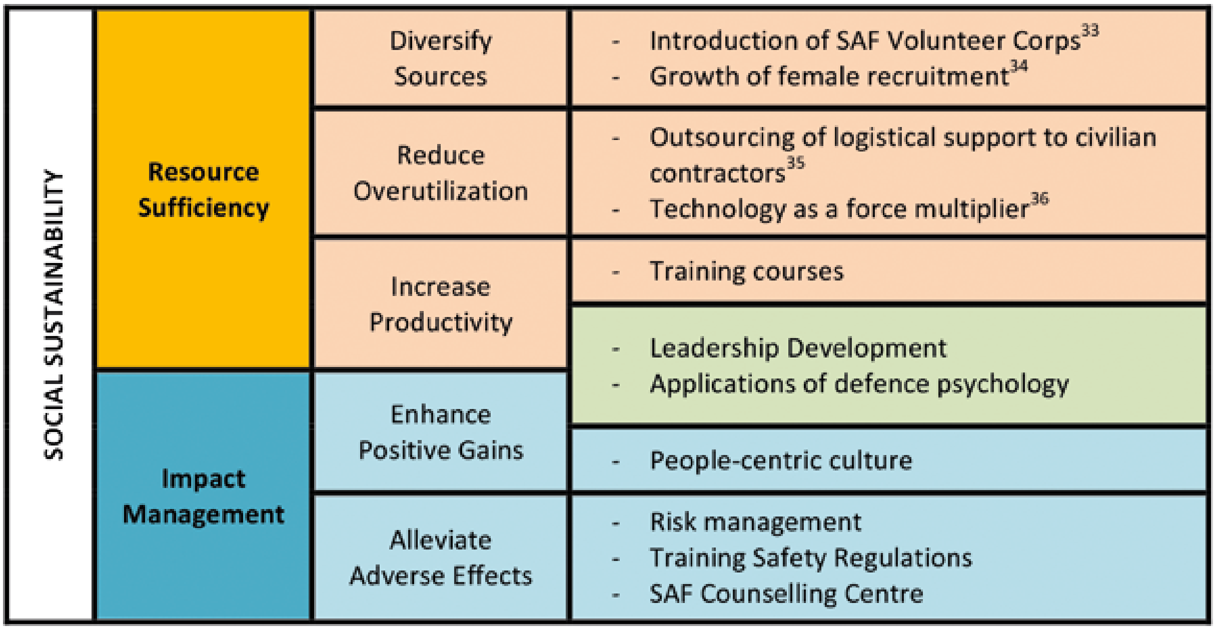
First, the social dimension is focused on the most important asset in the SAF—our people. It encompasses training, leadership development, safety, manpower policies for recruitment and retention, as well as instilling a sense of purpose, shared values and common identity into every serviceman/woman. By inspiring the commitment and maximising the potential of each individual, the SAF develops a resilient and competent workforce, with a people-centric culture. In this regard, considerable progress has been made over the years through an increased focus on people development. Project CARDINAL in the Air Force was a clear initiative to steer this.[29] Table 1 below summarises existing policies and structures within the SAF that promote social sustainability under the various strategies identified.

In addition, it is worth noting that the SAF is a 'key national institution' that plays a crucial role in strengthening our social fabric, and enlarging the 'common space' for a diversity of Singaporeans from different backgrounds.[30] The National Service experience of 'every Singaporean son' also has an impact on enhancing the social resilience of the Singaporean community at large.

By inspiring the commitment and maximising the potential of each individual, the SAF develops a resilient and competent workforce, with a people-centric culture.

ECONOMIC SUSTAINABILITY

The management of defence spending has always been done in a 'steady and prudent' manner.[31] In fact, sustainability has probably received the greatest focus in the economic domain, as the Ministry of Defence (MINDEF) has ensured consistent investments for the long-term sustainability of the defence budget, to avoid a 'feast and famine' approach.[32] It is useful to note that the three main aspects of defence expenditure are manpower, operations and deployments, as well as capability



SOCIAL SUSTAINABILITY	**Resource Sufficiency**	Diversify Sources	- Introduction of SAF Volunteer Corps[33] - Growth of female recruitment[34]
		Reduce Overutilization	- Outsourcing of logistical support to civilian contractors[35] - Technology as a force multiplier[36]
		Increase Productivity	- Training courses
			- Leadership Development - Applications of defence psychology
	Impact Management	Enhance Positive Gains	- People-centric culture
		Alleviate Adverse Effects	- Risk management - Training Safety Regulations - SAF Counselling Centre

Table 1: Examples of Social Sustainability Initiatives in the SAF

development (CAPDEV).[37] Hence, improvements in any of these areas through strategies in other domains may also contribute to financial cost reductions.

ENVIRONMENTAL SUSTAINABILITY

In the environmental arena, key natural resources required by the SAF include energy, water, food and land/sea space. As an example, consider how the SAF has accorded attention to resource sufficiency as a small island nation, with limited territorial space. This has allowed the SAF to not only support Singapore's economic activities and protect our sea lines of communication, but also maintain sufficient training areas. By diversifying sources, the SAF has gained access to training areas overseas, through defence arrangements and Memoranda of Understanding with other countries. Furthermore, the intention to relocate Paya Lebar Air Base illustrates an attempt to increase land space efficiency and 'enhance the effectiveness and resilience of the air bases', by expanding and replacing current facilities in Changi Air Base (East) and Tengah Air Base.[38] Without compromising operational readiness, the SAF makes way for Singapore's other residential and commercial land use needs. In this case, some efforts to reduce military utilisation of space may be done within the SAF, but planning of the overall land use also requires collaboration with external parties, such as the Urban Redevelopment Authority and Ministry of National Development.[39] This reiterates the need for inter-agency and, at times, multi-national efforts to promote sustainability.

Looking towards impact management instead, some of the main environmental outputs in the SAF include waste generation, pollution and noise. One key area that has been actively managed is that of noise generation, particularly aircraft jet noise over populated areas.

This also has a direct impact on operations as flying activities are ceased during certain periods to minimise disruption to the local community.[40] While techniques like flight path planning have been used for noise abatement, there are ways the SAF can continue to explore harnessing noise reduction technologies. Technology like acoustic liners in engines can play a critical role in improving noise efficiency, without necessarily reducing aircraft performance.[41] This may allow the SAF to reduce undesirable noise impacts for Singapore's population, without compromising mission effectiveness, and may even result in fewer restrictions and more flexible periods for flying.

MOVING FORWARD IN SUSTAINABILITY

ROLE OF TECHNOLOGY

One may then ask, "Where do our weapon systems fit in to all this? Are they not a resource too?" Indeed, on a tactical mission level, they may be seen as a resource along with troops and basic living necessities, to achieve the mission objective. However, on a broader level, they are part of the larger SAF ecosystem, utilising resource inputs like energy and manpower to be operated whilst generating output such as spent cartridges and carbon emissions, similar to the jet engine. They can be viewed as the technology that the SAF invests in, via our CAPDEV initiatives.

A common theme throughout the SAF's development is the use of technology as a force multiplier, also reflected in the SAF2030 vision.[42] Technology does have significant potential to enhance sustainability for the SAF, if capitalised on with the right intentions. As mentioned previously, technology can alleviate manpower pressures. For instance, unmanned systems may be used not only in the traditional sense of replacing manned aircraft platforms or troops on the ground (mules/humanoids), but also to supplement current operations in reconnaissance, thereby eliminating fatigue and safety considerations for 'dull, dirty and dangerous’ tasks. The greater autonomy achieved with improved control and software technologies also reduce the amount of manpower required for sustaining operations.

However, technology may also intensify the strain on resources by increasing resource demand. For example, by 2030, the number of Army units operating vehicular platforms is expected to almost double, increasing the mobility of our land forces.[43] Yet, with greater dependency on mechanised platforms and computer systems, the SAF will also have higher energy and cooling requirements. This would contribute to the depletion of resources, possibly causing a series of ripple effects, with indirect impacts to national security. Concurrently, the increased reliance on resources like fuel and energy creates a heightened risk of supply disruption, not only in its generation, but also in its storage and transfer.[44] This has a direct implication on mission effectiveness, especially with the growth of unconventional security threats like terrorism.

ENERGY RESOURCE SUFFICIENCY

The energy dependency of the military has increased in parallel with the changing characteristics of warfare, as evolution of military technology has moved into the ‘age of automation.’[45] The quantity of energy consumption has increased from 1 gallon per soldier per day in World War II (WWII) to 4 gallons per soldier per day during Operation Desert Storm in 1991, and one can only imagine how much more it has increased since.[46] This is not only on the base level infrastructure, but also on an individual level. For example, the Advanced Combat Man System (ACMS) equips ‘tactical units with network capabilities’ through its personal radio, communication keypad, portable computer, head-mounted display, weapon interactor and remote sensors.[47] However, this also implies that soldiers have to carry battery packs to power the various devices, which may well be the critical component for functioning of the overall system. Ensuring resource sufficiency in the SAF’s energy consumption is therefore crucial, and is a useful example to illustrate how technology can be harnessed.

The energy dependency of the military has increased in parallel with the changing characteristics of warfare, as evolution of military technology has moved into the ‘age of automation

First, energy sources can be diversified, by developing new, lasting primary energy sources, as the SAF’s platforms largely depend on ‘oil-based liquid fuel in one form or another.’[48] A shift towards renewable energies like solar power on buildings and wave energy at sea is not a dream for the future, but viable alternatives to be implemented. The United States (US) Department of Defense already has a biofuel programme making progress in allowing Air Force aircrafts and the Navy’s fleet to use alternative fuels without hindering operations, and possibly bring about cost benefits in the future.[49] Pushing technology further, novel energy harvesting techniques could be used on an individual level. A piezoelectric device can generate electrical energy from the kinetic energy of the mechanical motion of the soldier, and used to power the ACMS, for instance.[50] Technology is a very powerful instrument for exploring new energy sources.

Second, energy efficiency can be increased through suitable designs and energy efficient choices. As a simple example, compact fluorescent lightbulbs or light emitting diodes can be used in place of traditional incandescent ones.[51] While seemingly insignificant in small quantities, gains in efficiency can accumulate to larger energy savings. Design of buildings can also be optimised to maximise natural lighting and allow efficient airflow for ventilation. The Headquarters Combat Service Support Command (HQ CSSCOM) was constructed with such features, along with solar panels on the roof and rainwater recycling, thus achieving significant energy savings.[52]

Finally, energy consumption can be reduced by conservation. This can be done with simple technologies like motion-activated sensors for lighting. In addition to technology, increased awareness and positive practices can also contribute to reducing energy dependency without great cost, like switching off computers and other appliances when not in use. However, it should be recognised that such savings are small in comparison to an activity with larger consumption, such as commuting across the island from one base/camp to another for meetings. Carpooling or making economical travel plans when possible, for example, will significantly conserve more energy. With the right mindset and a little effort, adapting our lifestyles can help to reduce energy consumption.

ENVIRONMENTAL IMPACT MANAGEMENT

Beyond capitalising on technology, other tools can be used to enhance sustainability in the SAF. To minimise the adverse effects of our systems, a life-cycle analysis can be performed on the various technologies used by the SAF.[53] This should be done not only in terms of cost considerations in defence procurements, but also in terms of environmental impact from the initial procurement to final retirement of the system.[54] This evaluates the impact throughout a product's lifetime, and identifies the most critical stages for which suitable mitigation measures can then be implemented. At a more everyday level, some negative effects of waste generation can often be mitigated by establishing good practices, like indenting appropriate quantities of food in the cookhouse or encouraging the recycling of paper, metals and plastics in camps. Undoubtedly, there are difficulties in doing so, associated with convenience or expediency. As such, implementing structures to minimise the effort required to recycle, for instance, may allow sustainable practices to be inculcated as a form of habit or part of a routine, thereby reducing environmental footprint. Such initiatives have already begun in other militaries, such as the Israel Defence Forces (IDF).[55]

Internationally, militaries have also started to participate in discussions on sustainability. In 2009, the UN Environment Programme held a meeting on environmental norms and military activities in Geneva, attended by many states including Israel, Japan and the US.[56] Amongst other issues, the military's contribution to environmental policies for sustainable development and environmental impacts of military activities were reviewed. It is never too late for the SAF to look towards sustainability.

CONCLUSION

The SAF is instrumental to Singapore's development—not only in enhancing security, but also in contributing to the community. In the face of emerging security threats, SAF operations have evolved beyond a traditional defence role. Although seemingly counter-intuitive, the concept of sustainability is inherently linked to that of national security, and presents a useful way of thinking. By investing in resource sufficiency and impact management, the SAF can embrace the uncertainties of our complex security landscape and better position itself to protect Singapore's national interests. Achieving this, however, is no mean feat. Besides utilising technology as a tool to enhance sustainability, the SAF ultimately requires innovation and the collective effort of its people to drive any changes. After all, many aspects of our daily lives are like the jet engine—processes with inputs and outputs. If we see these processes through the eyes of sustainability and find the means to streamline them, via the strategies discussed or otherwise, the SAF will be well underway to start enhancing sustainability and optimising performance. The value of sustainability for the SAF, and consequently, for Singapore, is priceless.

BIBLIOGRAPHY

Abraham, Martin AA., ed. Sustainability Science and Engineering: Defining Principles. Vol. 1. Amsterdam: Elsevier, 2006.

Ashby, Michael F., Hugh Shercliff, and David Cebon. Materials: Engineering, Science, Processing and Design. Butterworth-Heinemann, 2013.

Brundtland, Gru, et al. "Report of the World Commission on Environment and Development: Our Common Future." 1987.

Caballero-Anthony, Mely, and Goh Tian. "ASEAN's Haze Shroud: Grave Threat to Human Security." RSIS Commentary 207 (5 Oct 2015). https://www.rsis.edu.sg/ rsis-publication/nts/co15207-aseans-haze-shroud-grave-threat-to-human-security/#.VsiVPzY -_eI

Chow, Jermyn. "SAF aims to Recruit At Least 500 More Women by 2018." The Straits Times. 21 Jul 2013. http://www.straitstimes.com/singapore/saf-aims-to-recruit-at-least-500-more-women-by-2018

CNA Military Advisory Board, "National Security and the Threat of Climate Change," The CNA Corporation (2007).

DSTA. "Channel Newsasia.com: Singapore's Ability to Plan Ahead Puts it in Good Stead." 23 March 2007. https://www.dsta.gov.sg/news-events/dsta-in-the-news/dsta-in-the-news---2007/channel-newsasia-com---23-march

Dwyer, Jim. "A National Security Strategy that Doesn't Focus on Threats." The New York Times, 3 May 2011. http://www.nytimes.com/2011/05/04/nyregion/a-strategy-for-national-security-focused-on-sustainability.html?_r=0

Ellis, Aurora. "Review: 'The Ultimate Weapon is No Weapon'." Foreign Policy in Focus. Institute for Policy Studies. 30 Aug 2010. http://fpif.org/review_the_ ultimate_weapon_is_no_weapon/

Energy Saving Trust. Energy Efficient Lighting. 2014. http://www.energysavingtrust .org.uk/domestic/energy-efficient-lighting

Feng, Zengkun. "Johor Reservoir's Water Level at Historic Low." The Straits Times. 4 Aug 2015. http://www.straitstimes.com/singapore/environment/johor-reservoirs-water -level-at-historic-low

González, José Luis, Antonio Rubio, and Francesc Moll. "Human Powered Piezoelectric Batteries to Supply Power to Wearable Electronic Devices." International Journal of the Society of Materials Engineering for Resources 10.1 (2002): 34-40. https://www.researchgate.net/publication/228542873_Human_Pow ered_Piezoelectric_Batteries_to_Supply_Power_to_Wearable_Electronic_Devices

Goodland, Robert. "Sustainability: Human, Social, Economic and Environmental." Encyclopedia of Global Environmental Change. John Wiley & Sons (2002).

Goodland, Robert. "The Concept of Environmental Sustainability." Annual Review of Ecology and Systematics 26 (1995): 1–24.

Hartman, James, et al. Sustainability and National Security. Carlisle: Centre for Strategic Leadership United States Army War College, January 2012.

Hill, Timothy E. "Focus on the Future – Institutionalising Sustainability into the Army." Engineer 38 (July-December 2008): 44-47.

Holland, Andrew, and Nick Cunningham. Fact Sheet: DoD's Biofuels Program. Washington DC: American Security Project, January 2013. http://www.americansecurityproject.org/dods-biofuels-program/

Israel Defense Forces, "Dreaming Green: IDF Takes Strides in Environmental Conservation," 6 May 2013. http://www.idf.il/1283-19112-en/Dover.aspx

IUCN, UNEP, and WWF. "Caring for the Earth: A Strategy for Sustainable Living." Gland, October 1991.

Kennedy, Caitlyn and Rebecca Lindsay. What's the Difference between Global Warming and Climate Change. climate.gov. 17 Jun 2015. https://www.climate.gov/ news-features/climate-qa/whats-difference-between-global-warming-and-climate-change

Lassa, Jonatan Anderias. "Zika Risk Governance and Climate Change." RSIS Commentary 29 (5 Feb 2016). https://www.rsis.edu.sg/rsis-publication/nts/co16029 -zika-risk-governance-and-climate-change/#.VsnJMDY-_eI

Leading in the Third Generation SAF. POINTER Monograph No 9 (July 2012).

Lim, Rachael. "Camp Green." Cyberpioneer. 11 Jan 2012. http://www.mindef. gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2012/jan12_fs2.html#.VssTFTY-_eJ

Mackay, David J.C. Sustainable Energy – Without the Hot Air. Cambridge: UIT Cambridge, 2009. http://www.withouthotair.com

Manohara, Chinniah. "Defence Procurement in Singapore." The DISAM Journal (2000): 86-94. http://www.disam.dsca.mil/ pubs/v.23_1/manohara.pdf

MINDEF. "Fact Sheet: Advanced Combat Man System." Official Release, 10 Oct 2012. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2012/oct/10oct12_nr2/10oct12_fs.html#.VssDtTY-_eI

MINDEF. "Management of Aircraft Noise." FAQs, 2 Jul 2013. http://www.mindef. gov.sg/imindef/press_room/faqs/faqaircraftnoise.html#.VsnqWjY-_eI

MINDEF. "Reply by Minister for Defence Dr Ng Eng Hen to Parliamentary Question on Singapore's Declining Birth Rate and Impact to the Singapore Armed Forces." Official Release, 12 Nov 2012. http://www.mindef.gov.sg/imindef/press_room/ official_releases/ps/2012/12nov12_ps.html#.VsmlqjY-_eI

MINDEF. "Reply by Minister for Defence Dr Ng Eng Hen to Parliamentary Question on Relocation of Paya Lebar Air Base." Official Release, 16 Sep 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/ps/2013/16sep13_ps.html#.VsjgkDY-8yE

MINDEF. "Reply to Media Queries on Army's Outsourcing of Logistical Support to Civilian Contractors." Official Release, 22 Dec 2014. http://www.mindef.gov.sg/ imindef/press_room/official_releases/mq/2014/22dec14_mq.html#.VsmrIzY-_eI

MINDEF. "SAF Deploys to Assist Indonesia to Fight Haze." Official Release, 10 Oct 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2015/oct/10oct15_nr.html#.VshmjDY-_eI

MINDEF. "Speech by Dr Ng Eng Hen, Minister for Defence, at Committee of Supply Debate 2014." Official Release, 6 Mar 2014. http://www.mindef.gov.sg/ imindef/press_room/official_releases/sp/2014/06mar14_speech.html#.VsxocTY-_eI

MINDEF. "Speech by Dr Tony Tan Keng Yam, Deputy Prime Minister and Minister for Defence, at the Opening Ceremony of THE CHEVRONS." Official Release, 8 Feb 2002. http://www.mindef.gov.sg/content/imindef/press_room/official_releases/ sp/2002/08feb02_speech.html#.Vsyo9TY-_eI

MINDEF. "Speech by Minister for Defence Teo Chee Hean, at Committee of Supply Debate 2009." Official Release, 12 Feb 2009. http://www.mindef.gov.sg/ imindef/press_room/official_releases/nr/2009/feb/12feb09_speech/12feb09_speech3.html#.VsjXrjY-_eI

MINDEF. "The SAF Adjusts Activities According to Haze Situation." Official Release, 15 Sep 2015. http://www.mindef.gov.sg/imindef/press_room/ official_releases/nr/2015/sep/15sep15_ nr.html#.VshmjjY-_eI

Ministry of National Development. A High Quality Living Environment for All Singaporeans: Land Use Plan to Support Singapore's Future Population. January 2013. http://www.mnd.gov.sg/landuseplan/e-book/#/12/

Mooney, Chris. "The Hidden Environmental Factors behind the Spread of Zika and other Devastating Diseases." The Washington Post. 3 Feb 2016. https://www.washingtonpost.com/news/energy-environment/wp/2016/02/03/the-hidden-environmental-factors-behind-the-spread-of-zika-and-other-deadly-diseases/?postshare=4231454600442677&tid=ss_tw

Morin, Cory W., Andrew C. Comrie, and Kacey Ernst. "Climate and Dengue Rransmission: Evidence and Implications." Environmental Health Perspectives 121.11-12 (2013): 1264. http://ehp.niehs.nih.gov/1306556/

National Climate Change Secretariat. Impact of Climate Change on Singapore. Prime Minister's Office Singapore. 22 Jan 2016. https://www.nccs.gov.sg/climate-change-and-singapore/national-circumstances/impact-climate-change-singapore

National Security Coordination Secretariat. "Addendum to the President's Address by Mr Teo Chee Hean, Deputy Prime Minister and Coordinating Minister for National Security." Prime Minister's Office Singapore. 2016. http://www.nscs.gov.sg/public/download. ashx?id=351

National Security Coordination Secretariat. "Opening Address by Deputy Prime Minister, Coordinating Minister for National Security and Minister for Home Affairs, Mr Teo Chee Hean, at the 12th National Security Seminar (NSS) on Wednesday 15 Oct 2014 at 9.30 am at the Hilton Hotel Singapore." Prime Minister's Office Singapore. http://www.nscs.gov.sg/public/download.ashx?id=332

Ong, Hong Tat. “Dr Ng showcases SAF2030 at Budget Debate.” Cyberpioneer. 7 Mar 2014. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/ articles/news/2014/mar/07mar14_news.html#.VsoHpzY-_eI

Ong, Wei Chong. “Singapore’s Defence Spending: A Long-Term Approach.” RSIS Commentary 6 (13 Jan 2010). https://www.rsis.edu.sg/rsis-publication/idss/1296-singapores-defence-spending/#.VsjWEDY-_eI

Porter, Gareth. “Environmental Security as a National Security Issue.” Current History. 94.592 (1995): 218-222. http://search.proquest.com/docview/200716223? accountid= 9851

Porter, Wayne, and Mark Mykleby. A National Strategic Narrative. Washington DC: Woodrow Wilson International Centre for Scholars, 2011.

Saritas, Ozcan, and Serhat Burmaoglu, "Future of Sustainable Military Operations under Emerging Energy and Security Considerations." Technological Forecasting and Social Change (2015).

Singapore Government. Defence Spending. MINDEF. 30 June 2015. http://www.mindef.gov.sg/imindef/key_topics/defence_spending.html

Singapore Government. Ministry of the Environment and Water Resources. http://www.mewr.gov.sg

Singapore Government. The Singapore Water Story. Public Utilities Board. 8 Jan 2016. http://www.pub.gov.sg/water/Pages/singaporewaterstory.aspx

Singapore Government. Urban Redevelopment Authority. https://www.ura.gov.sg/uol/

Singapore Government. Waste Minimisation and Recycling, National Environment Agency. 1 Feb 2016. http://www.nea.gov.sg/energy-waste/3rs

Southgate, Laura. “Indonesia’s Haze Crisis Fuels Southeast Asian Quarrel.” Global Risk Insights. 1 Oct 2015. http://globalriskinsights.com/2015/10/indonesia-haze-fuels-regional-quarrel/

Sustainable Development Commission. What is Sustainable Development. http://www.sd-commission.org.uk/pages/what-is-sustainable-development.html

Tang, Gareth, et al. “Future Energy and Power Challenges.” DSTA Horizons. 2009. https://www.dsta.gov.sg/docs/publications-documents/future-energy-and-power-challenges.pdf?sfvrsn=0

Teo, Benita. “SAF Volunteer Corps Launches Recruitment.” Cyberpioneer. 12 Oct 2014. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles /news/2014/oct/12oct14_news.html#.VsmohzY-_eJ

Teo, Esther. “Straits Times: S’pore gets Permanent Observer Status.” Ministry of Foreign Affairs Singapore Headlines. 16 May 2013. http://www.mfa.gov.sg/content/ mfa/media_centre/singapore_headlines/2013/201305/news_20130516.html

Teo, Jing Ting. “SAF 2030 Sneak Peek.” Cyberpioneer. 1 Feb 2016. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2016/feb16_fs1.html#.Vsn6xjY-_eI

U.S. Army. “U.S. Army Publishes Energy Security and Sustainability Strategy.” News Archive Article, 1 Jun 2015. http://www.army.mil/article/148559/U_S__Army_Publishes_Energy_Security_and_Sustainability_Strategy/

United Nations Environment Programme, “International Meeting on Environmental Norms and Military Activities: Notification by the Secretariat.” http://www.unep.org/ delc/Portals/119/pdf/InternationalmeetingDec09-notification.pdf

Virginia Tech. “Researchers seek to Reduce Ear-Splitting Jet Engine Noise.” Phys.org. 19 Mar 2013. http://phys.org/news/2013-03-ear-splitting-jet-noise.html

ENDNOTES

1. Gru Brundtland, et al., "Report of the World Commission on Environment and Development: Our Common Future," 1987.

2. Sustainable Development Commission, What is Sustainable Development. http://www.sd-commission.org.uk/pages/what-is-sustainable-development.html

3. UCN, UNEP, and WWF, “Caring for the Earth: A Strategy for Sustainable Living,” (Gland, Switzerland, October 1991).

4. For example, the US Army released a roadmap known as the Energy Security and Sustainability (ES2) Strategy. U.S. Army, “U.S. Army Publishes Energy Security and Sustainability Strategy,” News Archive Article, 1 Jun 2015. http://www.army.mil/article/148559/U_S__Army_Publishes_Energy_Security_and_Sustainability_Strategy/

5. Robert Goodland, "Sustainability: Human, Social, Economic and Environmental," Encyclopedia of Global Environmental Change, John Wiley & Sons (2002).

6. National Security Coordination Secretariat, “Addendum to the President’s Address by Mr Teo Chee Hean, Deputy Prime Minister and Coordinating Minister for National Security,” Prime Minister’s Office Singapore, 2016. http://www.nscs.gov.sg/public/ download.ashx?id=351

7. The causes of climate change will not be discussed in this essay, but readers who are interested can read more on the website of the Intergovermental Panel on Climate Change (IPCC) at http://www.ipcc.ch.

8. Gareth Porter, "Environmental Security as a National Security Issue," Current History, 94.592 (1995): 218-222. http://search.proquest.com/docview/200716223?accountid= 9851

   CNA Military Advisory Board, "National Security and the Threat of Climate Change," The CNA Corporation (2007).

9. James Hartman, et al., Sustainability and National Security (Carlisle: Centre for Strategic Leadership United States Army War College, January 2012).

10. Caitlyn Kennedy and Rebecca Lindsay, What's the Difference between Global Warming and Climate Change, climate.gov, 17 Jun 2015. https://www.climate.gov/news-features/climate-qa/whats-difference-between-global-warming-and-climate-change

11. Zengkun Feng, "Johor Reservoir's Water Level at Historic Low," The Straits Times, 4 Aug 2015. http://www.straitstimes.com/singapore/environment/johor-reservoirs-water-level-at-historic-low

12. Singapore Government, The Singapore Water Story, Public Utilities Board, 8 Jan 2016. http://www.pub.gov.sg/water/Pages/singaporewaterstory.aspx

13. Esther Teo, "Straits Times: S'pore gets Permanent Observer Status," Ministry of Foreign Affairs Singapore Headlines, 16 May 2013. http://www.mfa.gov.sg/content/mfa/media_centre/singapore_headlines/2013/201305/news_20130516.html

14. National Climate Change Secretariat, Impact of Climate Change on Singapore, Prime Minister's Office Singapore, 22 Jan 2016. https://www.nccs.gov.sg/climate-change-and-singapore/national-circumstances/impact-climate-change-singapore

15. CNA Military Advisory Board, "National Security and the Threat of Climate Change," The CNA Corporation (2007).

16. Cory W. Morin, Andrew C. Comrie, and Kacey Ernst, "Climate and dengue transmission: evidence and implications," Environmental Health Perspectives 121.11-12 (2013): 1264. http://ehp.niehs.nih.gov/1306556/

    Chris Mooney, "The Hidden Environmental Factors behind the Spread of Zika and other Devastating Diseases," The Washington Post, 3 Feb 2016. https://www.washingtonpost.com/news/energy-environment/wp/2016/02/03/the-hidden-environmental-factors-behind-the-spread-of-zika-and-other-deadly-diseases/?postshare=4231454600442677&tid=ss_tw

17. This is a common criticism against environmental problems as a national security issue. Gareth Porter, "Environmental Security as a National Security Issue." (see endnote 9)

18. Mely Caballero-Anthony, and Goh Tian, "ASEAN's Haze Shroud: Grave Threat to Human Security," RSIS Commentary 207 (5 Oct 2015). https://www.rsis.edu.sg/rsis-publication/nts/co15207-aseans-haze-shroud-grave-threat-to-human-security/#.VsiVPzY -_eI

19. MINDEF, "The SAF Adjusts Activities According to Haze Situation," Official Release, 15 Sep 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2015/ sep/15sep15_nr.html#.VshmjjY-_eI

20. MINDEF, "SAF Deploys to Assist Indonesia to Fight Haze," Official Release, 10 Oct 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2015/oct/10oct15_nr.html#.VshmjDY-_eI

21. Laura Southgate, "Indonesia's Haze Crisis Fuels Southeast Asian Quarrel," Global Risk Insights, 1 Oct 2015. http://globalriskinsights.com/2015/10/indonesia-haze-fuels-regional-quarrel/

22. National Security Coordination Secretariat, "Opening Address by Deputy Prime Minister, Coordinating Minister for National Security and Minister for Home Affairs, Mr Teo Chee Hean, at the 12th National Security Seminar (NSS) on Wednesday 15 Oct 2014 at 9.30 am at the Hilton Hotel Singapore," Prime Minister's Office Singapore. http://www.nscs.gov.sg/ public/download.ashx?id=332

23. Jim Dwyer, "A National Security Strategy that Doesn't Focus on Threats," The New York Times, 3 May 2011. http://www.nytimes.com/2011/05/04/nyregion/a-strategy-for-national-security-focused-on-sustainability.html?_r=0

24. This paper was written by Retired U.S. Marine Col. Mark Mykleby and U.S. Navy CAPT. Wayne Porter, intended to guide national policy decisions. Wayne Porter, and Mark Mykleby, A National Strategic Narrative, (Washington DC: Woodrow Wilson International Centre for Scholars, 2011).

25. Gru Brundtland, et al., "Our Common Future." (see endnote 1)

26. Singapore Government, Ministry of the Environment and Water Resources. http://www.mewr.gov.sg

27. Singapore Government, Waste Minimisation and Recycling, National Environment Agency, 1 Feb 2016. http://www.nea.gov.sg/energy-waste/3rs

28. Timothy E. Hill, "Focus on the Future – Institutionalising Sustainability into the Army," Engineer 38 (July-December 2008): 44-47.

29. Leading in the Third Generation SAF, POINTER Monograph No 9 (July 2012).

30. MINDEF, "Speech by Dr Tony Tan Keng Yam, Deputy Prime Minister and Minister for Defence, at the Opening Ceremony of THE CHEVRONS," Official Release, 8 Feb 2002. http://www.mindef.gov.sg/content/imindef/press_room/official_releases/sp/2002/08feb02_speech.html#.Vsyo9TY-_eI

31. Singapore Government, Defence Spending, MINDEF, 30 June 2015. http://www.mindef. gov.sg/imindef/key_topics/defence_spending.html

32. MINDEF, "Speech by Minister for Defence Teo Chee Hean, at Committee of Supply Debate 2009," Official Release, 12 Feb 2009. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2009/feb/12feb09_speech/12feb09_speech3.html#.VsjXrjY-_eI

    Wei Chong Ong, "Singapore's Defence Spending: A Long-Term Approach," RSIS Commentary 6 (13 Jan 2010). https://www.rsis.edu.sg/rsis-publication/idss/1296-singapores-defence-spending/#.VsjWEDY-_eI

33. Benita Teo, "SAF Volunteer Corps Launches Recruitment," Cyberpioneer, 12 Oct 2014. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/oct/12oct14_news.html#.VsmohzY-_eJ

34. Jermyn Chow, "SAF aims to Recruit At Least 500 More Women by 2018," The Straits Times, 21 Jul 2013. http://www.straitstimes.com/singapore/saf-aims-to-recruit-at-least-500-more-women-by-2018

35. MINDEF, "Reply to Media Queries on Army's Outsourcing of Logistical Support to Civilian Contractors," Official Release, 22 Dec 2014. http://www.mindef.gov.sg/imindef/press_room/official_releases/mq/2014/22dec14_mq.html#.VsmrIzY-_eI

36. "High Mobility Artillery Rocket System (HIMARS) needs only 3 men to fully operate the system compared with 12 men needed for other artillery systems with less precision and destructive effects. For the Navy, the Formidable-class frigates needs a full complement of about 70 men, a very lean crew compared to similar warships from other navies, which typically operate with about 100 men. The recently acquired Heron-1 Unmanned Aerial Vehicle (UAV) also gives us greater aerial surveillance capabilities for the same number of people deployed, as compared to older UAVs."

    MINDEF, "Reply by Minister for Defence Dr Ng Eng Hen to Parliamentary Question on Singapore's Declining Birth Rate and Impact to the Singapore Armed Forces," Official Release, 12 Nov 2012. http://www.mindef.gov.sg/imindef/press_room/official_ releases/ps/2012/12nov12_ps.html#.VsmlqjY-_eI

37. Singapore Government, Defence Spending, MINDEF, 30 June 2015. http://www.mindef.gov.sg/imindef/key_topics/defence_spending.html

38. MINDEF, "Reply by Minister for Defence Dr Ng Eng Hen to Parliamentary Question on Relocation of Paya Lebar Air Base," Official Release, 16 Sep 2013. http://www.mindef.gov.sg/imindef/press_room/official_releases/ps/2013/16sep13_ps.html#.VsjgkDY-8yE

39. Singapore Government, Urban Redevelopment Authority. https://www.ura.gov.sg/uol/

    Ministry of National Development, A High Quality Living Environment for All Singaporeans: Land Use Plan to Support Singapore's Future Population (January 2013). http://www.mnd.gov.sg/landuseplan/e-book/#/12/

40. MINDEF, "Management of Aircraft Noise," FAQs, 2 Jul 2013. http://www.mindef.gov.sg/imindef/press_room/faqs/faqaircraftnoise.html#.VsnqWjY-_eI

41. Acoustic liners usually consist of a honeycomb layer with a porous sheet. They help to attenuate noise by absorbing the acoustic energy at a design frequency and dissipating it as heat and other energy forms.

42. Jing Ting Teo, "SAF 2030 Sneak Peek," Cyberpioneer, 1 Feb 2016. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2016/feb16_fs1.html#.Vsn6xjY-_eI

43. Hong Tat Ong, “Dr Ng showcases SAF2030 at Budget Debate,” Cyberpioneer, 7 Mar 2014. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/ news/2014/mar/07mar14_news.html#.VsoHpzY-_eI

44. Ozcan Saritas, and Serhat Burmaoglu, "Future of Sustainable Military Operations under Emerging Energy and Security Considerations." Technological Forecasting and Social Change (2015).

45. bid.

46. Ibid.

47. MINDEF, “Fact Sheet: Advanced Combat Man System,” Official Release, 10 Oct 2012. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2012/oct/10oct12_nr2/10oct12_fs.html#.VssDtTY-_eI

48. Gareth Tang, et al., “Future Energy and Power Challenges,” DSTA Horizons, 2009. https://www.dsta.gov.sg/docs/publications-documents/future-energy-and-power-challenges.pdf?sfvrsn=0

49. Andrew Holland, and Nick Cunningham, Fact Sheet: DoD’s Biofuels Program, (Washington DC: American Security Project, January 2013). http://www.americansecurityproject.org/dods-biofuels-program/

50. José Luis González, Antonio Rubio, and Francesc Moll, “Human Powered Piezoelectric Batteries to Supply Power to Wearable Electronic Devices,” International Journal of the Society of Materials Engineering for Resources 10.1 (2002): 34-40. https://www.researchgate.net/publication/228542873_Human_Powered_Piezoelectric_Batteries_to_Supply_Power_to_Wearable_Electronic_Devices

51. Energy Saving Trust, Energy Efficient Lighting, 2014. http://www.energysavingtrust. org.uk/domestic/energy-efficient-lighting

52. achael Lim, “Camp Green,” Cyberpioneer, 11 Jan 2012. http://www.mindef.gov.sg/ imindef/resourcelibrary/cyberpioneer/topics/articles/features/2012/jan12_fs2.html#.VssTFTY-_eJ

53. Michael F. Ashby, Hugh Shercliff, and David Cebon, Materials: Engineering, Science, Processing and Design, Butterworth-Heinemann, 2013.

54. DSTA uses a Life Cycle Management (LCM) methodology to evaluate costs of the defence system through its entire lifetime, such as infrastructure, logistics, manpower and maintenance, in addition to the initial procurement cost. Chinniah Manohara, “Defence Procurement in Singapore,” The DISAM Journal (2000): 86-94. http://www.disam.dsca.mil/pubs/v.23_1/manohara.pdf

    DSTA, “Channel Newsasia.com: Singapore’s Ability to Plan Ahead Puts it in Good Stead,” 23 March 2007. https://www.dsta.gov.sg/news-events/dsta-in-the-news/dsta-in-the-news---2007/channel-newsasia-com---23-march

55. Israel Defense Forces, “Dreaming Green: IDF Takes Strides in Environmental Conservation,” 6 May 2013. http://www.idf.il/1283-19112-en/Dover.aspx

56. United Nations Environment Programme, “International Meeting on Environmental Norms and Military Activities: Notification by the Secretariat.” http://www.unep.org/delc/Portals/119/pdf/InternationalmeetingDec09-notification.pdf

LTA Julie Lim Yee Sin is a pilot trainee currently undergoing Basic Wings Course in 130 SQN. A recipient of the SAF Merit Scholarship, LTA Julie graduated from the University of Cambridge in 2016 with a Master of Engineering and Bachelor of Arts in Engineering (Aerospace and Aerothermal).

MARITIME TERRORISM THREAT IN SOUTHEAST ASIA AND ITS CHALLENGES

by ME6 Joses Yau Meng Wee

Abstract:

The threat of terrorism is always present, but the public was only given a wake-up call to the devastating impacts of terrorism after the September 11 attacks in the United States (US). Since then, many countries have stepped up their counter-terrorism efforts and measures. For example, the Association of Southeast Asian Nations (ASEAN) adopted a comprehensive approach to improve the regional security. In this essay, the author examines the terrorism threat in Southeast Asia, exploring the possible scenarios of a maritime terrorist attack in the region and thoroughly assesses the region's counter-terrorism efforts that have been put in place. The author also introduces an Opportunity, Capability and Intent (OCI) framework as a form of threat assessment, to affirm his stand that the terrorist threat in Southeast Asia is indeed very real.

Keywords: Terrorism; Counter-terrorism; Efforts and Measures; Regional Security; Threat Assessment

INTRODUCTION

The September 11 attacks in the US underscored the devastating effects of terrorism to the world. The attacks on *USS Cole* in 2000, *MV Limburg* in 2002, *SuperFerry* 14 in 2004 and the *M Star* in 2010 are classified as acts of 'Maritime Terrorism', a stark reminder that the world's waterways continue to be vulnerable. The maritime environment has some attributes that, on a basic level, could very well be conducive for terrorist activities to occur (e.g., the legal immunity in relation to activities on high seas, poor or conflicting efforts by numerous countries in trying to establish a safe operating environment in coastal regions and port facilities). Furthermore, maritime terrorist attacks have the potential to cause mass casualties, interruption to global trade as well as extreme damage to property.

This essay seeks to ascertain a common definition of 'Maritime Terrorism' and followed on to affirm that the terrorism threat in Southeast Asia is real through the use of the Opportunity, Capability and Intent (OCI) threat assessment framework. Next, the essay will discuss eight probable scenarios of a maritime terrorist attack in Southeast Asia and attempt to examine the credibility of each scenario. Finally, the essay will assess the adequacy of the region's counter-terrorism efforts, highlighting the need to take a regional approach to combat extremist ideology.

HOW REAL IS THE THREAT OF MARITIME TERRORISM IN SOUTHEAST ASIA?

DEFINITION OF 'MARITIME TERRORISM'

So what exactly is the definition of 'Maritime Terrorism'? Unfortunately, the 1982 United Nations Convention on the Law of the Sea Treaty (UNCLOS)

Wikipedia

The USS Cole after the al-Qaeda suicide attack on the 12th October, 2000.

was not particularly clear about what constitutes 'Maritime Terrorism', the closest being the definition of Piracy under Article 101. As such, the definition advocated by the Council for Security Cooperation in the Asia Pacific (CSCAP) was adopted in this paper. CSCAP states that 'Maritime Terrorism' is defined as:

> *'...the undertaking of terrorist acts and activities (1) within the maritime environment, (2) using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, (3) against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities.'*[1]

OPPORTUNITY, CAPABILITY, INTENT

The terrorism threat in Southeast Asia is real and I will use the OCI threat assessment framework to elaborate further. 'Opportunity' refers to how easy it is for terrorists to conduct their activities. 'Capability' addresses the know-how and ability of terrorist organisations to carry out their actions and 'Intent' refers to their resolve to follow through those actions.

OPPORTUNITY

Southeast Asia is one of the world's busiest and strategic chokepoints, accounting for approximately 40% of the total global maritime trade.[2] With numerous ships passing by each day, the opportunity to hijack a ship to use as a weapon or carry out attacks (e.g., planting a bomb) on-board ships remains high.

The situation is further exacerbated by the fact that commercial shipping is a complex multinational network. A ship could be flagged in one country but owned by a company based in another country. Its crew can consist of a mix of nationals and its cargo can be consigned by numerous companies from all over the world transiting through the territorial waters of a third country heading towards a port of a fourth country. Given such complexity and ease of access to move people and goods in the maritime domain, the opportunities for terrorists to conduct their activities continues to exist.

CAPABILITY

In terms of hardware, terrorists continue to employ low-cost explosive devices against their targets. Notwithstanding, the ease of access to these raw materials as well as dual-use technologies such as satellite communication systems, Global Positioning System, recreational maritime vehicles (e.g., yacht, fast boats and jet skis) increases the available inventory that maritime terrorists can exploit to advance their cause.[3]

Terrorists have also been known to align themselves to criminal organisations in order to gain access to the required expertise and resources, both in terms of manpower as well as financial support through activities such as smuggling and money laundering.[4] Terrorist organisations have also exploited the use of social media and internet forums to recruit manpower, spread their ideology and teach the techniques, tactics and procedures (TTP) in carrying out terrorist acts. Given that some countries continue to be plagued by endemic income inequality and corruption, these factors have fuelled the growth of extremists within the region and spurned more radicalised individuals to join these terrorist organisations.[5]

INTENT

Terrorism works at the mental and psychological levels by imparting and spreading trepidation in their casualties. The mere threat of an attack is sufficient to trigger governments into a host of arrangements to deter and disrupt terrorism. In the information operations realm, the successful assaults completed by Al Qaeda since 2000 had encouraged their members, regional terrorist organisations (e.g., the Kumpulan Militan Malaysia (KMM), Jemaah Islamiyah (JI), Abu Sayyaf Group, Moro Islamic Liberation Front, Laskar Jihad, Gerakan Aceh Merdeka, more recently, Jamaah Ansharusy Syariah) and 'Lone Wolves' to carry out high pay-off returns in the maritime domain.[6] For example, the attack by Abu Sayyaf Group in 2004 on the *SuperFerry 14* in the Philippines saw 116 passengers killed.[7]

No doubt, these terrorist organisations continue to publicise their intent, rallying supporters to join their cause and encouraging them to carry out attacks. For example, in 2002, Singapore managed to uncover reconnaissance information gathered by JI on US naval facilities and ships based in Singapore. In May 2015, ISIS renewed calls to attack Singapore, Philippines and the US, following the disruption of a terrorist cell in Malaysia in April 2015 which had intentions of carrying out bomb attacks in Putrajaya.[8] In May 2015, Singapore's Ministry of Home Affairs detained a 19 year old student who had intentions to join ISIS in Syria and failing which, may have attempted to carry out 'Lone Wolf' attacks.[9] Such evidence continues to demonstrate that the threats to our maritime security are real, present and clear.

POSSIBLE SCENARIOS OF A MARITIME TERRORIST ATTACK IN SOUTHEAST ASIA

To understand the dangers of maritime terrorism, there is a need to examine the list of vulnerabilities and potential outcomes that can be connected to potential attacks. This analysis must be grounded on authentic information and insights to the capabilities as well as goals of terrorist organisations. The Rand Corporation, in its study *'Maritime Terrorism - Risk and Liability'* recognised seven conceivable scenarios where maritime terrorism might happen.[10] Trend Micro completed a risk assessment study in December 2014 and highlighted eight potential scenarios that may be exploited by terrorists. The eight scenarios are as follows:

Scenario 1

Smuggle Chemical, Biological, and Radiological, Explosive (CBRE) materials ashore via cargo containers to carry out attacks at significant commercial ports such as Hong Kong or Singapore or key targets on land.[11]

With more than 100 million cargo containers being moved through the world's ports each year, it is possible that terrorists may choose to smuggle their CBRE materials in one of these containers. The sheer volume alone means that it is not feasible to carry out a 100% check on all the cargo containers.[12]

Notwithstanding, another area of concern is the robustness of supply chains. The multifaceted and complex nature of freight shipment in ports represents another weak link to the security issue. Cargo is loaded at one area and transported by truck or rail to a port and thereafter, loaded onto a ship where it gets transferred to another ship at a transhipment port before reaching its destination. To ensure that the supply chain network is not compromised and all phases of the supply chain are screened, a significant amount of investment from the logistics as well as transport industry is required.[13] However, all these measures drive up overheads and time needed to move goods. Thus, it is unlikely that the developing countries in Southeast Asia will be willing to incur these costs unless it is a universal requirement by all ports to comply.

Scenario 2

Use of 'Trojan Horse' tactics, concealing weapons or other explosive devices, in seemingly harmless looking vessels as such fishing trawlers, tugs or re-supply ships.

Not only does the International Ship and Port Facility Security (ISPS) Code exclude vessels less than 500 tons, it also provides exclusion for all fishing vessels regardless of their size. Notwithstanding, a number of international standards that are applicable to merchant vessels are not applicable to the fishing vessels found in Southeast Asia, in part due to their haphazard operations schedule as well as the limited number of qualified seafarers on-board.[14] Likewise, there have been numerous cases in which the vessel's crew records were conflicting or erroneous. What this means is that these vessels continue to be the preferred choice for the conduct of illicit activities such as smuggling of weapons in hidden compartments under a boat load of fish. As these vessels are not Safety of Life at Sea (SOLAS)-compliant, security initiatives such as those implemented by Singapore (i.e., Harbour Craft Transponder System, Harbour Craft Security Code, and Ship Self Security Assessment Checklist) can be implemented by regional Port State Controls to deter maritime terrorism.[15] The Mumbai attack is an example where terrorists exploited a seemingly harmless fishing vessel to bypass security agencies.

Scenario 3

Hijacking a vessel as a means to raise funds or to support their crusade of political viciousness co-ordinated toward ethnic, ideological, religious, or separatist outlines.

In 1985, the *MS Achille Lauro* was hijacked by four members of the Palestine Liberation Front (PLF).[16] The hijackers demanded the release of 50 Palestinians locked up in Israeli jails. The incident saw one Jewish American passenger being killed in response to negotiation breakdown.[17] In 2001, *MT Tri Samudra*, a chemical tanker, carrying a full cargo of inflammable petrochemical products, was hijacked by 35 gunmen, likely from the Free Aceh Movement, in Malacca Straits. The ship and crew were released, supposedly upon payment of the ransom.[18] While these hijacks involved the smaller vessels, such as product tankers, tugs and fishing trawlers, they are largely carried out by criminal organisations that have the means to off load the valuable cargo on-board.

Wikipedia/ D. R. Walker

On 7th October, 1985, four men representing the Palestine Liberation Front (PLF) hijacked the Italian MS Achille Lauro liner off the coast of Egypt, as she was sailing from Alexandria to Ashdod, Israel.

Scenario 4

Scuttling a ship at a chokepoint or narrow Sea Lines of Communication (SLOC) (e.g., Malacca Straits) to disrupt commercial trade and shipping movement.

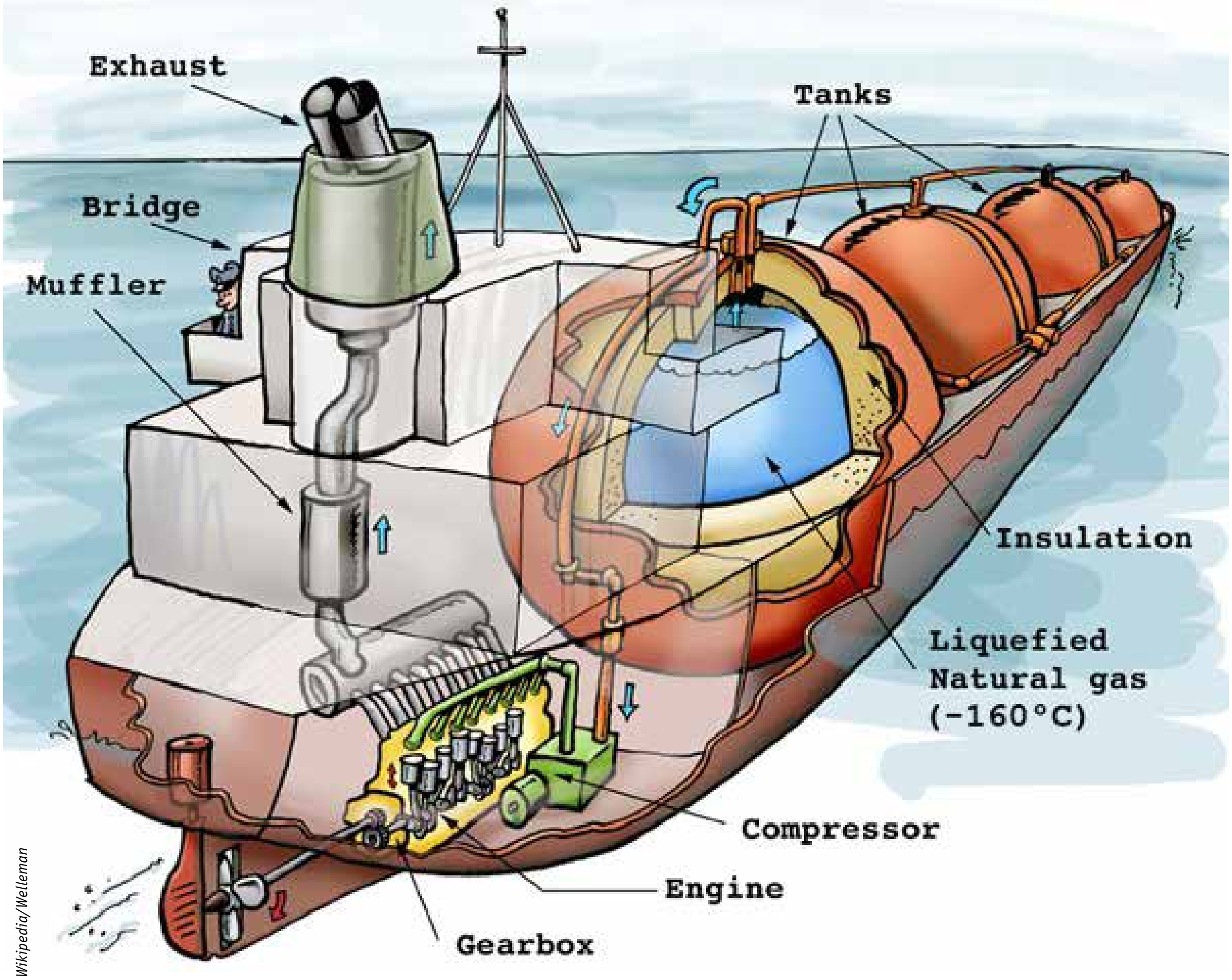
Looking at the context of Southeast Asia, in particular the Malacca Straits, it is highly unlikely that such an attack will achieve its intended outcome. This is because at One Fathom Bank, or the narrowest point in Malacca Straits, it is approximately 0.6 nautical miles wide and ships can circumvent round the sunken ship and continue on their passage.[19] However, the threat from mines or floating Improvised Explosive Devices (IEDs) is far greater and will achieve the intended outcome of disrupting shipping movement in a SLOC.[20]

Scenario 5

Hijacking a Liquefied Natural Gas (LNG) carrier and then exploding it as a floating bomb or utilising it as an impact weapon against port facilities.

Large vessels have long stopping distances and if used as an impact weapon against a port facility, can cause significant destruction. When these vessels are carrying high-risk or inflammable goods such as LNG, terrorists could hijack these ships and use them as floating bombs to target port facilities.[21]

Natural Gas is not explosive in its liquid state. That is why refrigerated tankers are used to store huge amounts of LNG for transportation. However, once it is exposed to the ambient environment, LNG rapidly evaporates and forms an ignitable cloud.[22] When this cloud is ignited, the heat generated is capable of melting steel at a separation distance of



Wikipedia/Welleman

Layout of a typical LNG Carrier.

about 1,200 feet away.[23] A fire of such magnitude will be difficult to put out and can only be extinguished when all its fuel has been spent. For a port like Singapore, the effect of such an incident will be decimating. Death toll and serious infrastructure damage is expected to be high at the impact point as well as in the vicinity. This would also imply that the port would need to work at a decreased limit, resulting in delays and a loss of business. That said, the complexities in carrying out such an attack would render the threat from an LNG carrier to be low. It is easier to exploit more combustible platforms such as chemical tankers or Liquefied Petroleum Gas carriers to achieve the intended effect.[24]

The disruption of oil trade as a result of a terrorist attack will have significant implications to the emerging economies of Southeast Asia.

Scenario 6

Use of small powerboats to assault an oil tanker or oil terminal to influence global petroleum costs or create significant contamination in the coastal areas.

The attack on *M/V Limburg* and *M Star* demonstrated the vulnerability of large ocean-going vessels in out-manoeuvring small powerboats. It also showed the difficulty in causing critical damage to these huge vessels if the impact is not correlated with the vessel's structural weak points. Notwithstanding, terrorists have continued to use small powerboats to assault oil terminals in an attempt to destabilise a country. For instance, the attacks on the Al Basrah and Khor Al Amaya oil terminal in Iraq back in 2004 caused both terminals to be shut down for two days, resulting in lost revenues of approximately US$40 million.[25] The disruption of oil trade as a result of a terrorist attack will have significant implications to the emerging economies of Southeast Asia. In addition, the potential for the contamination of coastal areas in Southeast Asia increases in tandem with the number of ships transporting oil through the region.[26]

Scenario 7

Create mass casualty situation on-board a cruise ship or passenger ferry by detonating a bomb on-board or using a small but fast boat laden with explosives to ram the ship.

Terrorists can disguised themselves as tourists to gain access to cruise ships and plant explosives in order to trigger a mass casualty situation. For example, the Abu Sayyaf group's attack on the *SuperFerry 14* in 2004 was carried out by detonating 20 sticks of explosives that were stored inside an emptied out TV set. As a result, a fire broke out and 116 passengers were killed.[27] In 2005, Lu'ai Sakra, an al Qaeda–linked organisation utilised a small boat laden with high explosives and smashed it into an Israeli cruise ship carrying travellers destined for Turkey.[28]

Scenario 8

Using cyber attacks to hijack or spoof Automatic Identification System (AIS) transponder codes.

Trend Micro evaluated the AIS installed on-board ships and concluded that the system is susceptible to hijacking, disruption as well as spoofing.[29] For instance, Closest Point of Approach (CPA)-spoofing can fake a possible collision scenario and cause the targeted ship to veer off-course and run aground. AIS-Search and Rescue transponder (SART) spoofing could potentially lure Search and Rescue (SAR) vessels into a trap laid by terrorists. AIS hijacking could potentially trigger conflicts between nations by 'moving' military ships into another nation's territorial waters.

ARE THE REGIONAL COUNTER-TERRORISM ARRANGEMENTS SUFFICIENT?

ASEAN members have, since 9/11, adopted a comprehensive approach to improve the regional security through continued informal interactions and focusing on economic development. In order to deter, detect and disrupt terrorism, a combination of security, economic and ideological measures are required at the national level. In addition, ASEAN members have collaborated with one another in the fight against terrorism by improving the geopolitical climate between countries through confidence building measures, shared intelligence, capacity building and enhancing interoperability.[30] This section will elaborate on the regional arrangements established in combating terrorism and propose that greater collaboration between regional countries is required to combat terrorism at its source, by defeating its ideology.

In order to deter, detect and disrupt terrorism, a combination of security, economic and ideological measures are required at the national level.

Confidence Building Measures

At the geopolitical level, there is great value in enhancing co-operation between states, building trust and strengthening relationships. Such acts will result in the building up of 'maritime capital', allowing states to utilise this resource in times of crisis. To achieve this, ASEAN members have put in place numerous platforms and initiatives to enhance maritime security. For example, forums such as the ASEAN Regional Forum, ASEAN Defence Ministers' Meeting (ADMM) and the ADMM-Plus Maritime Security Working Group continue to provide opportunities for collaboration towards peace and security in Southeast Asia.[31]

Shared Intelligence

In addition, co-operation between Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) Information Sharing Centre, Information Fusion Centre (IFC), regional intelligence agencies, navies, coast guards and more importantly, the inclusion of the shipping community themselves, have been effective in combating maritime terrorism. Given the finite resources available to the navies and enforcement agencies, the Head of UK Maritime Trade Operations (UK MTO) office in Dubai suggested at the Regional Maritime Security Practitioner Course (RMPC) 2015 that greater co-operation and leadership be displayed by the militaries in tapping the thousands of sensors (i.e., commercial ships) that transit through the region for ground intelligence on potential threats to maritime security. For instance, the perpetrators responsible for the hijack of oil tanker *V.L.14* off the South China Sea on 28th August, 2014 were successfully interdicted within 16 hours through the collaboration between regional agencies.[32] That said, collective sense making continues to be relevant to overcome the limitation of finite resources that each country has. With the use of advanced data analytics tools, trend lines can be ascertained and priority of interception can be tagged to ships traversing from high risk states or those with links to terrorist organisations. Such pre-emptive measures serve to deter, detect disrupt terrorist acts even they arrive at their destination.[33]

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

Capacity Building and Enhancing Interoperability

Concerted capacity building activities continued to be conducted by IFC. They include the annual Regional Maritime Security Practitioner Course (RMPC) and the international maritime information-sharing workshops/exercises. Notwithstanding, the conduct of multilateral maritime exercises at sea and ashore continues to strengthen information exchanges and interoperability between navies and maritime agencies, enabling them to respond decisively when called upon.[34] Such exercises include the Maritime Information Sharing Exercise (MARISX), Western Pacific Naval Symposium (WPNS) Multilateral Sea Exercise (WMSX), Exercise Bersama Shield and Exercise Bersama Lima under the Five Power Defence Arrangement as well as the biennial Rim of Pacific Exercise (RIMPAC). Last but not the least, security arrangements like the Malacca Strait Patrols and the adoption of the Code for Unplanned Encounters at Sea (CUES) continue to foster co-operation between navies in tackling threats to regional maritime security.[35]

CHALLENGES TO REGIONAL COUNTER-TERRORISM EFFORTS

While the region's efforts have been effective in deterring, detecting and disrupting maritime terrorism, there exist challenges to the conduct of good order at sea and terrorists are likely to exploit these gaps. As argued by Sam Bateman, these challenges can be summarised into five main points: (1) presence of sovereignty and/or boundary disputes; (2) lack of clearly defined and mutually agreed maritime boundaries between coastal states; (3) lack of capacity and coordination within the national maritime administrators; (4) lack of support for key maritime treaties (e.g., International Convention on Maritime Search and Rescue (SAR) and Suppression of Unlawful Acts (SUA) and (5) regional differences in interpreting the law of the sea with regards to territorial rights, duties and exclusive economic zones.[36]

Many legal challenges will continue to arise in the fight against maritime terrorism. As such, it is important for regional states to refrain from eroding or damaging the incumbent Law of the Sea by adopting unilateral practices and claiming it to be 'international customary law' to advance their own interests.[37] The lack of a common definition of 'Maritime Terrorism' will also continue to undermine the region's efforts in achieving effective governance and co-operation in the maritime domain.

ADDRESSING THE ROOT CAUSE OF TERRORISM

In order to defeat terrorism, there is a need to address the fundamental social and political issues as well as to remove the financing support that allows terrorists to procure weapons and other related materials. While peace and security amongst regional states in Southeast Asia has propelled the region to economic success over the past decade, it is equally important not to be too focused on the 'hard' approaches to defeat terrorism. 'Hard' approaches such as safeguarding targets, capturing terrorists and sharing knowledge will not be adequate to defeat terrorism. There is a need for regional countries to collaborate with one another and adopt 'soft' approaches that target the ideology of radical Islamists and win the hearts and minds of progressive Islamists in Southeast Asia.[38]

While peace and security amongst regional states in Southeast Asia has propelled the region to economic success over the past decade, it is equally important not to be too focused on the 'hard' approaches to defeat terrorism.

CONCLUSION

ASEAN's political endeavours and co-operation over the past decade have eliminated crevices in the law that provided safe haven for terrorists to operate. Regional efforts as well as whole-of-government approach to combat terrorism have achieved the effects of deterring, detecting and disrupting terrorism. But the work is not done.

This essay has established that the maritime terrorism threat in Southeast Asia is real and the terrorist organisations have the opportunity, capability and intent to carry out the attacks. The eight possible scenarios were explained in the context of Southeast Asia with the latest addition of cyber attacks on the AIS following the study done by Trend Micro. Finally, the essay analysed ASEAN's efforts in fighting terrorism and acknowledged that confidence building measures, shared intelligence, capacity building and enhancing interoperability have been effective in deterring, detecting and disrupting maritime terrorism. The essay also highlighted five main challenges that may undermine these efforts and propose greater regional collaboration in combating radical Islamist ideology.

BIBLIOGRAPHY

Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. "A security evaluation of AIS automated identification system." In Proceedings of the 30th Annual Computer Security Applications Conference, pp. 436-445. ACM, 2014.

Bateman, Sam. "The Future Maritime Security Environment in Asia: A Risk Assessment Approach." Contemporary Southeast Asia: A Journal of International and Strategic Affairs 37, no. 1 (2015): 49-84.

Bateman, W. S. G., Joshua Ho, and Mathew Mathai. "Shipping patterns in the Malacca and Singapore straits: an assessment of the risks to different types of vessel." Contemporary Southeast Asia: A Journal of International and Strategic Affairs 29, no. 2 (2007): 309-332.

Blomberg, S. Brock, Khusrav Gaibulloev, and Todd Sandler. "Terrorist group survival: ideology, tactics, and base of operations." Public Choice 149, no. 3-4 (2011): 441-463.

Cui, Yifang. "Dangerous goods regulating system in Singapore." (2010).

Desker, Barry. "Islam in Southeast Asia: the challenge of radical interpretations." Cambridge review of international affairs 16, no. 3 (2003): 415-428.

Emmers, Ralf. "Comprehensive security and resilience in Southeast Asia: ASEAN's approach to terrorism 1." The Pacific Review 22, no. 2 (2009): 159-177.

Franco Joseph and Quivooij Romain. “Terrorist Threats from the Maritime Domain: Singapore’s Response” (2015).

Gaouette, Mark. Cruising for trouble: Cruise ships as soft targets for pirates, terrorists, and common criminals. ABC-CLIO, 2010

Graham, Euan. "Maritime Security and Threats to Energy Transportation in

Southeast Asia." The RUSI Journal 160, no. 2 (2015): 20-31.

Greenberg, Michael D., Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz. Maritime terrorism: risk and liability. Rand Corporation, 2006

Gunaratna, Rohan. "Al Qaeda’s origins, threat and its likely future." Terrorism in the Asia-Pacific: Threat and Response (2003): 145.

Halberstam, Malvina. "Terrorism on the high seas: the Achille Lauro, piracy and the IMO convention on maritime safety." American Journal of International Law (1988): 269-310.

Kaplan, Eben. "Liquefied Natural Gas: A Potential Terrorist Target?." Council on Foreign Relations 8 (2006)

Lorenz, Akiva J. "Al Qaeda's maritime threat." International Institute for Counter-Terrorism 17 (2007).

Partridge, Amy Roach. "Scrutinizing supply chain security." Inbound Logistics 32, no. 1 (2012).

Quentin, Sophia. "Shipping Activities: Targets of Maritime Terrorism." MIRMAL, Vol. 2, (2003) http://www.derechomaritimo.info/pagina/mater.htm

Raj, Andrin. "Japan’s initiatives in security cooperation in the straits of Malacca on maritime security and in Southeast Asia: piracy and maritime terrorism." The Japan Institute for International Affairs. Retrieved March 31 (2009): 2012.

Raymond, C. "Maritime terrorism, a risk assessment: The Australian example." Joshua Ho and Catherina Zara Raymond, eds (2005).

Raymond, Catherine Zara. "Maritime Terrorism in Southeast Asia: Potential Scenarios." Terrorism Monitor 4, no. 7 (2006): 1-2.

Raymond, Catherine Zara, and Arthur Morriën. "1 Security in the Maritime Domain and Its Evolution Since 9/11." of Maritime Security (2008): 1.

Sheng, Hong Sheng. "Legal Aspects of the Prevention and Suppression of Maritime Terrorism in the Asia-Pacific Region." Korean journal of defense analysis 24, no. 1 (2012): 107-122.

"19-year-old Detained for Planning to Join ISIS Had Planned to Kill President and PM Lee." The Straits Times / Singapore. May 29, 2015. Accessed June 11, 2015. http://www.straitstimes.com/news/singapore/more-singapore-stories/story/19-year-old-detained-planning-join-isis-had-planned-kill.

"Bomb Caused Philippine Ferry Fire." BBC News. October 11, 2004. Accessed June 11, 2015. http://news.bbc.co.uk/2/hi/asia-pacific/3732356.stm.

“ISIS social media post cites Singapore as possible target.” The Straits Times / Singapore. May 29, 2015. Accessed June 11, 2015. http://www.straitstimes.com/news/singapore/more-singapore-stories/story/isis-social-media-post-cites-singapore-possible-target-2

"Malaysian Military Warns Underwater Mines Could Be Terrorist Tool." DefenceTalk. June 7, 2006.. Accessed June 11, 2015. https://www.defencetalk.com/malaysian-military-warns-underwater-mines-could-be-terrorist-tool-6414/

"Radical Islam Movement Changes Focus, Lacks Leadership." The Jakarta Post. February 18, 2015. Accessed June 11, 2015. http://www.thejakartapost.com/news/2015/02/18/radical-islam-movement-changes-focus-lacks-leadership.html.

"Speech by Minister of State for Defence, Dr Mohamad Maliki Bin Osman, at the Simultaneous Special Session 4 on "Regional Security in the Gulf and the Indo-Pacific", India Global Forum." Singapore Government. November 9, 2014. Accessed June 11, 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2014/09nov14_speech.html#.VXqdKUYavz8.

"Speech by Minister for Defence Dr Ng Eng Hen at the Third IISS Fullerton Forum: The Shangri-La Dialogue Sherpa Meeting." Singapore Government. January 26, 2015. Accessed June 11, 2015.

Jennings, Mr Peter. "Maritime Confidence Building Measures in the South China Sea Conference." (2013). http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/26jan15_speech.html#.VXqdjkYavz8.

ENDNOTES

1. Quentin, Sophia. "Shipping Activities: Targets of Maritime Terrorism." MIRMAL, Vol. 2, (2003) http://www.derechomaritimo.info/pagina/mater.htm

2. Graham, Euan. "Maritime Security and Threats to Energy Transportation in Southeast Asia." The RUSI Journal 160, no. 2 (2015): 20-31.

3. Raymond, C. "Maritime terrorism, a risk assessment: The Australian example." Joshua Ho and Catherina Zara Raymond, eds (2005).

4. Lorenz, Akiva J. "Al Qaeda's maritime threat." International Institute for Counter-Terrorism 17 (2007).

5. Gunaratna, Rohan. "Al Qaeda's origins, threat and its likely future." Terrorism in the Asia-Pacific: Threat and Response (2003): 145.

6. Desker, Barry. "Islam in Southeast Asia: the challenge of radical interpretations." Cambridge review of international affairs 16, no. 3 (2003): 415-428.

   "Radical Islam Movement Changes Focus, Lacks Leadership." The Jakarta Post. February 18, 2015. Accessed June 11, 2015. http://www.thejakartapost.com/news/2015/02/18/radical-islam-movement-changes-focus-lacks-leadership.html.

7. "Bomb Caused Philippine Ferry Fire." BBC News. October 11, 2004. Accessed June 11, 2015. http://news.bbc.co.uk/2/hi/asia-pacific/3732356.stm.

8. "ISIS social media post cites Singapore as possible target." The Straits Times / Singapore. May 29, 2015. Accessed June 11, 2015. http://www.straitstimes.com/news/singapore/more-singapore-stories/story/isis-social-media-post-cites-singapore-possible-target-2.

9. "19-year-old Detained for Planning to Join ISIS Had Planned to Kill President and PM Lee." The Straits Times / Singapore. May 29, 2015. Accessed June 11, 2015. http://www.straitstimes.com/news/singapore/more-singapore-stories/story/19-year-old-detained-planning-join-isis-had-planned-kill.

10. Greenberg, Michael D., Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz. Maritime terrorism: risk and liability. Rand Corporation, 2006

11. Ibid.

12. Ibid.

13. Partridge, Amy Roach. "Scrutinizing supply chain security." Inbound Logistics 32, no. 1 (2012).

14. Bateman, W. S. G., Joshua Ho, and Mathew Mathai. "Shipping patterns in the Malacca and Singapore straits: an assessment of the risks to different types of vessel." Contemporary Southeast Asia: A Journal of International and Strategic Affairs 29, no. 2 (2007): 309-332

15. Cui, Yifang. "Dangerous goods regulating system in Singapore." (2010).

16. Halberstam, Malvina. "Terrorism on the high seas: the Achille Lauro, piracy and the IMO convention on maritime safety." American Journal of International Law (1988): 269-310.

17. The Achille Luaro incident subsequently led to the creation of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) in 1988.

18. Raymond, Catherine Zara. "Maritime Terrorism in Southeast Asia: Potential Scenarios." Terrorism Monitor 4, no. 7 (2006): 1-2.

19. If for some reasons, the terrorists is able to scuttle multiple ships and effectively blocked the Malacca Straits, what this means is that vessels will be forced to bypass Malacca Straits and use either Lombok or Sunda Straits to reach their destinations, potentially incurring additional shipping costs and delays but not resulting in a standstill of maritime trade in the region

20. "Malaysian Military Warns Underwater Mines Could Be Terrorist Tool." DefenceTalk. June 7, 2006.. Accessed June 11, 2015. https://www.defencetalk.com/malaysian-military-warns-underwater-mines-could-be-terrorist-tool-6414/

21. Raj, Andrin. "Japan's initiatives in security cooperation in the straits of Malacca on maritime security and in Southeast Asia: piracy and maritime terrorism." The Japan Institute for International Affairs. Retrieved March 31 (2009): 2012.

22. It is not easy to create a cloud of fire on an LNG carrier. First, LNG carriers are designed with numerous safety provisions such as compartmentalizing the tanks to prevent contact with one another. In addition, the power needed to break the structure of the tank would more likely than not, cause fire at the tank area and light up the gas as it escapes into the surrounding, restricting the potential damage fairly to the LNG carrier. As such, it is unlikely that a cloud of fire can be created during such an attack.

23. Kaplan, Eben. "Liquefied Natural Gas: A Potential Terrorist Target?." Council on Foreign Relations 8 (2006)

24. Ibid.

25. Raymond, Catherine Zara, and Arthur Morriën. "1 Security in the Maritime Domain and Its Evolution Since 9/11." of Maritime Security (2008): 1.

26. In 1997, Singapore experienced the worst oil spill in its history when the oil tanker Evoikos collided with the Very Large Crude Carrier (VLCC) Orapin Global in the Singapore Straits. As a result of the collision, 25,000 tonnes of oil were spilled into the sea, generating enormous damage to the maritime environment

27. "Bomb Caused Philippine Ferry Fire." BBC News. October 11, 2004. Accessed June 11, 2015. http://news.bbc.co.uk/2/hi/asia-pacific/3732356.stm.

28. Gaouette, Mark. Cruising for trouble: Cruise ships as soft targets for pirates, terrorists, and common criminals. ABC-CLIO, 2010

29. AIS provides real-time tracking and monitoring information to enhance the safety of ships at sea. Since 2002, it has been installed onboard over 300,000 vessels. The AIS system has been used during search-and-rescue (SAR) operations as well as accident investigations. Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. "A security evaluation of AIS automated identification system." In Proceedings of the 30th Annual Computer Security Applications Conference, pp. 436-445. ACM, 2014.

30. Emmers, Ralf. "Comprehensive security and resilience in Southeast Asia: ASEAN's approach to terrorism 1." The Pacific Review 22, no. 2 (2009): 159-177.

31. "Speech by Minister of State for Defence, Dr Mohamad Maliki Bin Osman, at the Simultaneous Special Session 4 on "Regional Security in the Gulf and the Indo-Pacific", India Global Forum." Singapore Government. November 9, 2014. Accessed June 11, 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2014/09nov14_speech.html#.VXqdKUYavz8.

32. Sharing by Head IFC during RMPC 2015

33. Franco Joseph and Quivooij Romain. "Terrorist Threats from the Maritime Domain: Singapore's Response" (2015).

34. "Speech by Minister for Defence Dr Ng Eng Hen at the Third IISS Fullerton Forum: The Shangri-La Dialogue Sherpa Meeting." Singapore Government. January 26, 2015. Accessed June 11, 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/26jan15_speech.html#.VXqdjkYavz8.

35. Jennings, Mr Peter. "Maritime Confidence Building Measures in the South China Sea Conference." (2013).

36. Bateman, Sam. "The Future Maritime Security Environment in Asia: A Risk Assessment Approach." Contemporary Southeast Asia: A Journal of International and Strategic Affairs 37, no. 1 (2015): 49-84.

37. Sheng, Hong Sheng. "Legal Aspects of the Prevention and Suppression of Maritime Terrorism in the Asia-Pacific Region." Korean journal of defense analysis 24, no. 1 (2012): 107-122.

38. Blomberg, S. Brock, Khusrav Gaibulloev, and Todd Sandler. "Terrorist group survival: ideology, tactics, and base of operations." Public Choice 149, no. 3-4 (2011): 441-463.

ME6 Joses Yau currently holds a Master of Science in Physical Oceanography (Distinction) from Naval Postgraduate School in 2012 and was presented at the Naval Undersea Warfare Division Newport Award for Excellence in Undersea Warfare Technology. He pursued a part-time degree on his own and graduated from National University of Singapore with a Bachelor of Technology (Electronics Engineering) (2nd Class Honours, Upper Division) in 2004.

UNMANNED AERIAL VEHICLES AND THE FUTURE OF AIRPOWER: A TECHNOLOGICAL PERSPECTIVE

by ME4 Gerald Goh Qi Wen

Abstract:

Since the invention of the aeroplane by the Wright Brothers in 1903, developments in aerial space, particularly in airpower, have moved at a rapid pace. For countries whose militaries have developed a competent air force, airpower gives them a myriad of capabilities to protect their country's air space and security, such as the ability of airpower to access targets beyond the capabilities of the army and navy and to effectively destroy key infrastructure or high value targets with its penetration and range. Yet, with the advancement of weaponry such as Surface-to-Air missiles and Integrated Air Defence Systems, a more precise theorisation of airpower may be required to ensure the safety of a country's defence. This essay aims to give a technological perspective of the future of airpower, as well as a detailed analysis of unmanned aerial vehicles' role in operations today and its potential advantages and disadvantages.

Keywords: Unmanned Aerial Vehicles; Airpower; Technology; Integrated Air Defence System; Future

INTRODUCTION

TRADITIONAL AIRPOWER THEORY

Airpower comprises the use of flying vehicles to support a nation's security interests. There are myriad definitions of airpower. In this essay, the author will be considering two salient features of airpower that have been relevant for the majority of the 20th century and will remain relevant, albeit in different forms, in the future. The first feature, access, is the ability of airpower to access targets beyond the capabilities of land and maritime forces due to geographical limitations or static enemy defence. The penetration and range of airpower make the dynamics of its employment tactically and strategically effective in destroying key infrastructure and other high value targets. The second feature, speed, is the ability of airpower to amass quickly at a selected time and place, bringing to bear a concentrated amount of destructive force before appropriate evasive or defensive measures can be taken. These features mark the traditional notions of airpower as the ability of an air force to achieve air superiority, conduct strike operations and support other services.

REVIEW OF AIRPOWER THEORY FOR THE FUTURE

There is an urgent and fundamental need to revisit the concept of airpower for future threats and operating environments. With the advent of advanced Surface-to-Air Missiles, Integrated Air Defence System (IADS), and the introduction of Airborne Early Warning and stealth capabilities in our region, it may become increasingly impractical to depend on expensive and sophisticated manned platforms to achieve both strategic and tactical objectives.[1] The author will address the previous two features mentioned in traditional Airpower theory and propose the inclusion of strategic strike in a theorisation of future airpower.

ACCESS

The advanced surveillance and reconnaissance capabilities of the Republic of Singapore Air Force's (RSAF) Heron 1 UAV will prove to be important components in the complex battle environment of the future.

With the advancement of radar and sensors in addition to on-going developments of counter-stealth technology, only systems at the micro, near-silent and ultra-low energy levels will have any chance of operating undetected. Small Unmanned Aerial Vehicles (UAVs) that are extremely difficult to track and target, yet highly capable of both Intelligence, Surveillance and Reconnaissance (ISR) and offensive capabilities, have a higher chance of penetrating the network of sensors.[2] Another aspect of penetration could be achieved via sheer numbers, which would require autonomous UAVs which could be pre-programmed and execute their missions either with co-operative control (better known as 'swarm' technology) for maximum effect or for covert operations. Autonomous capability is a critical advantage for any military as it allows the system to react to threats faster with faster iterations within the decision-making loop. In addition, it should be noted that access is no longer restricted to geography, but should also be expanded to include communications and electronic networks as they play a greater role in warfare today and in the future.

Autonomous capability is a critical advantage for any military as it allows the system to react to threats faster with faster iterations within the decision-making loop.

SPEED

Aircraft speed was an important measure of capability as the speed envelope directly impacts manoeuvring in a tactical dogfight. It is also a key component of strategic bombers which could enter the Area of Operations (AO) at high altitude and speed, drop their payloads and escape before it can be detected and brought down by enemy air defences. However, modern detection and targeting capabilities render aircraft speed to be practically irrelevant. The traditional notion that a tactical advantage is achieved by physical speed should be revised to the speed of information gathering and more importantly, processing of the information into usable intelligence. The military force which can collect, exploit and disseminate these information faster will hold the tactical advantage and allow better decision-making in force employments, especially for time-critical targets. In other words, the speed at which the military force completes the ISR cycle will determine its ability to secure air superiority regardless of whether the eventual attack is carried out by aircraft, ground forces, and naval missiles or even through cyber attacks.

STRATEGIC STRIKE

The third feature to be introduced is the increasing importance of an effective strategic strike capability. With the steadily growing economy of developing countries in the region and their emphasis on force modernisation, it is a matter of time before other countries in the region will be able to afford more advanced assets in greater numbers, such as stealth fighters and IADS.[3] The wars waged by the United States (US) and Israel in the Middle East also highlighted the political costs of collateral damage and perceived imbalance of military force application. Hence, it is critical for air forces to develop the capability to conduct precise strike operations to achieve strategic effects with minimal collateral damage. Attacks on key targets in civilian areas may even require the use of non-kinetic weapons to minimise harm to infrastructure and humans. Persistent presence for target monitoring, recognition and opportune engagement becomes more important than purely payload size and accuracy.[4]

UAVS' ROLE IN OPERATIONS TODAY

Remotely piloted aircraft were used more than fifty years ago, however, the increasing usage of armed UAVs in recent years have evolved UAV roles beyond the traditional ISR functions.[5] Extensive use of armed UAVs began with Operation Enduring Freedom and Operation Iraqi Freedom.[6] The armed UAVs provided direct support of military operations and were mostly utilised to detect and kill al-Qaeda and Taliban leadership in Afghanistan and Iraq.

The use of UAVs in contested airspace is still premature as many of the Predators in Iraq were shot down by Iraqi MiGs due to its low speed and vulnerability. However, once air superiority was achieved, the use of UAVs for close air support proved to be effective. This was primarily due to its ability to loiter over the Area of Operations (AO), provide intelligence to ground commanders and accurately neutralise key threats with extended time over target. The use of UAVs had also reduced the sensor-shooter loop as the UAV pilot was able to seamlessly complete the Fix, Find, Track, Target, Engage, Assess (F2T2EA) loop for time critical targeting. Persistent tracking of key enemy movements also provided key intelligence and bought time for decision-making and strike packages to be prepared.

It is also observed that the acquisition and development of UAVs, both armed and unarmed, are on an upward trend for most military forces in the world. It is projected that spending on procurement and development will grow from US$6.6 billion in 2013 to US$11.4 billion in 2022.[7] However, only 23 out of 70 UAV users have developed or are developing armed UAVs.[8] Self-imposed export control by the American government and the alignment of most friendly nations are some of the main reasons why proliferation of armed UAVs is not widespread yet. However, other countries actively markets their armed UAVs, with China announcing publicly that it would be exporting its armed UAV, *Wing Loong*, to Saudi Arabia and other

Wikipedia/Baiweiflight

China's Wing Loong UAV.

unspecified countries.[9] Similarly, weaponising a UAV does not require extensive research. Less-developed countries such as Iran had created UAVs which could be used as 'suicide' weapons.[10] Faced with these realities, governments might have to review their export controls to friendly nations to counter these proliferation threats.

UAVS' AIRPOWER ROLE IN THE FUTURE

ENHANCED SPEED AND STRATEGIC STRIKE CAPABILITIES THROUGH PLATFORM AND PAYLOAD DEVELOPMENTS

Most militaries in the world are investing heavily in UAV technologies, and drone warfare will be the next bound in the evolution of airpower. The US, China and other developed nations are currently developing Unmanned Combat Aerial Vehicles (UCAVs) such as the Boeing X-45 and Sharp Sword. UCAVs can perform similar tasks as modern manned fighter aircraft with similar performance and self-defence features. Future UCAVs are likely to come with built-in autonomy, as demonstrated by the Northrop Grumman X-47B's capability of landing on an aircraft carrier, a challenging task even for aviation pilots.[11]

In terms of weapons, there are multiple trajectories in developments including micro-munitions, electromagnetic bombs, self-protection weapons and Directed Energy Weapons (DEWs). Electromagnetic bombs could be used to deliver a sharp burst of electromagnetic pulse which has the potential to destroy electronic targets without causing harm to infrastructure and humans. DEWs such as high-power microwave and high-energy laser are currently under development to exploit the long endurance of UAVs as they are effective for as long as the UAVs are in flight. This movement away from traditional munition-based weaponry will further increase the attractiveness of UAVs as a persistent ISR and strike asset which could achieve strategic strike effects with minimal collateral damage. Instead of employing speed to transit to the mission area quickly, UAVs are able to loiter over potential targets and strike on opportunity, leaving the targets with little reaction time.

In efforts to enable UAVs to match and even surpass current manned platforms, future UAVs such as the Northrop Grumman RQ-180 will incorporate stealth technologies to further reduce their radar cross-section, which are already small compared to manned platforms.[12] UAVs are also moving towards the use of turbofan engines, or in special cases, ramjets to attain speeds far greater than the turboprop or rotary power plants used in most UAVs today.[13] In the future, designers will have to trade speed and power performances with the traditional long endurance capability of UAVs today with consideration of an expansion of roles.

ENHANCED ACCESS AND STRATEGIC STRIKE CAPABILITIES THROUGH ELECTRONIC WARFARE

One of the upcoming capabilities for future UAVs that will enable Airpower to penetrate modern IADS is Electronic Warfare (EW). For example, the US Marine Corps tested the viability of UAVs to conduct EW missions against enemy air defences using MQ-9 Reapers carrying the Northrop Pandora EW System to carry out wideband, multifunctional jamming attacks on radar and targeting systems in support of tactical strike missions. UAVs are ideal EW systems due to the high-risk nature of close-in jamming or decoy operations and the ability to loiter over the area of operations for extended coverage. Systems such as the ADM-160 Miniature Air-Launched Decoy and the Northrop Grumman Bat come equipped with EW payloads to add on to their spectrum of missions, and are especially effective against Anti-Access/Area Denial (A2AD) strategies. As payloads get miniaturised in the future, as demonstrated by the Pandora system which was able to screen a fighter group in an attack package and was small enough to be integrated in a small tactical UAV, it will become increasingly easy and cheap for tactical ground commanders to employ EW capabilities. The low cost (asset and operating costs) of UAVs also enables the deployment of more assets in a single mission, allowing networked UAVs to operate as a swarm to provide suppression over large areas for specified times opening corridors for operations.

ENHANCED SPEED AND ACCESS THROUGH ACCURATE AND TIMELY INTELLIGENCE

To achieve accurate and timely intelligence, UAVs employ a suite of ISR payloads that includes Imagery Intelligence (IMINT), Communications Intelligence (COMINT) and Electronic Intelligence (ELINT). IMINT is critical in accomplishing Find, Fix, Track as part of the F2T2EA loop and commonly comprises fusion of multiple sensors such as Synthetic Aperture Radar (SAR) and Long Range Electro-Optics/Infra-Red (EO/IR) sensors. For EO/IR, one of the technologies being developed is the Wide Area Persistent Surveillance (WAPS) system, with an example being the Gorgon Stare system which was used in Afghanistan as a MQ-9 Reaper payload.[14] The WAPS system provides city-size images to provide a full field of view instead of a 'straw' view associated with traditional EO/IR sensors. WAPS aids in exploitation of pattern-of-life and is used to monitor and track multiple events of interest within a large area of operations, greatly enhancing the situational awareness of ground commanders.

The use of radars in UAVs for ISR is becoming commonplace, with the employment of SAR technology to deliver long-range and very high-resolution images and Ground Moving Target Indicator (GMTI) radars to detect moving targets against clutter. Developments are currently on-going for Foliage Penetration (FOPEN) technology, with an example being Lockheed Martin's Tactical Reconnaissance and Counter-Concealment system, which utilises a low-frequency dual band SAR to peer through foliage, rain and darkness and detect both moving and stationary targets. Multi-sensor fusion of FOPEN SAR, GMTI and ELINT enhances target identification in adverse conditions and aid in the targeting and engagement of high value assets. One of the challenging aspects of ISR is the need for substantial manpower and time to exploit the data that are collected, future developments of visual intelligence such as the Defense Advanced Research Projects Agency (DARPA)'s Mind's Eyewill enable automated analysis and detection of operationally significant activities.[15]

These MUAVs could potentially operate undetected for weeks and track targets through complicated terrain in urban areas. They could also be deployed for covert strike operations to disrupt key enemy installations or remote tagging or targeting for their larger counterparts to employ precision weapons.

In the future, with higher computing density and performance, more powerful COMINT and ELINT payloads will be able to be integrated within smaller UAV platforms. COMINT and ELINT sensors detect, geo-locate and classify Radio-Frequency transmissions and allow forces to access or disrupt enemy communications, these capabilities are key to enhancing the survivability of friendly forces whilst destroying/disrupting the enemy's military capabilities. Taiwan, for example, actively uses unmanned SIGINT aircraft to patrol the East China Sea to intercept the use of long range radars of China's A2AD systems.[16] In terms of ELINT, current payloads include Specific Emitter Identification and Automatic Identification System which greatly enhances situational awareness of the battle space in air, land and sea. The combination of these payloads and the UAV's ability to loiter and project these capabilities directly over the AO allow commanders to harness the tactical advantage derived from the speed of intelligence cycle and access to enemy networks.

GAME CHANGERS

Multi-UAV Control

There have been increasing interest and research into networked UAVs to perform complex tasks autonomously. The networking of multiple UAVs opens up a multitude of opportunities for mass operations that would have been otherwise too expensive or impractical to carry out with manned platforms. For example, there have been studies conducted into using UAVs which co-operate and explore a wide area quickly through datalink relay and dynamic task re-allocation. This can be controlled by a single pilot, allowing the military force to have a wider picture of the overall battle space with minimal human intervention. The co-operative control of these UAVs may even extend to the optimisation of targeting flight plans and perform co-ordination of multiple targets. The idea of using swarms of UAVs also potentially allows UAVs to overwhelm enemy air defences either by launching electronic attacks or by saturating the radar returns of detection systems. One other potential application is the creation of a mobile wireless mesh network which permits a group of UAVs to deploy large communication networks allowing ground forces to tap on images captured by any member of the swarm or utilise the network for ground communications.

Micro-UAVs

The most revolutionary aspect of UAVs in future warfare is the use of Micro-UAVs (MUAVs) in swarm operations. Currently, the United States Air Force (USAF) Research Laboratory is developing swarms of MUAVs based on biological fliers, such as birds and insects that could be mass-deployed via a larger aircraft. These could be used for extended surveillance in plain sight of the enemy and could extract key intelligence at extremely close ranges. Their endurance could also be extended through solar power or even the extraction of power from vibrating machinery or power lines. These MUAVs could potentially operate undetected for weeks and track targets through complicated terrain in urban areas. They could also be deployed for covert strike operations to disrupt key enemy installations or remote tagging or targeting for their larger counterparts to employ precision weapons. The ability of an MUAV to remain indefinitely in an AO while executing its missions autonomously could herald a new age in military technology.

POTENTIAL CHALLENGES FOR UAV AIRPOWER

Situational Awareness, Speed and Manoeuvrability

Lack of situational awareness is often quoted as a severe disadvantage of UAVs in air-to-air scenarios. UAV Pilots do not have the same field of vision as compared to pilots in a bubble canopy of modern tactical fighters; they can only rely on a suite of sensors to monitor the UAV's surroundings. UAV pilots are subjected to latency issues which could be significant for Within Visual Range (WVR) dogfights, which requires instantaneous decisions.[17] In the same vein, UAVs also perform worse off in terms of manoeuvrability and speed as compared to fighter aircraft. However, it can be argued that visual

The Sky Archer Counter Micro-UAV System is a locally developed solution to neutralise hostile and illegal drones within a 1km radius.

situational awareness may no longer be relevant with the proliferation of Beyond Visual Range (BVR) weapons today. In fact, situational awareness should be viewed as the ability to detect threats even before the threat becomes imminent through more advanced sensors and networked capabilities. Manoeuvrability and speed no longer remains relevant as the payload can be released or evasive actions can be taken way before the enemy detects the UAV. This will necessarily entail the miniaturisation of sensors or the use of overwhelming numerical advantage to match or overcome the more advanced electronic systems on board manned platforms or radar stations.

Lack of situational awareness is often quoted as a severe disadvantage of UAVs in air-to-air scenarios.

Payload Capacity

UAVs are currently disadvantaged in terms of payload capacity when compared to their manned counterparts. For example, the MQ-9 Reaper can carry a payload of 1,724 kg while the lightweight Northrop F-5 can carry a maximum payload of 3,175kg. This is mainly due to the nature of UAV design, which values endurance more than physical performance. The current UAV payload capacity limits their ability to dispense firepower or carry bulky EW systems. However, it must be clarified that the limitation was a result of the modality of current UAV operations which influenced its design. It is not farfetched to envisage UAVs that can carry as much payloads as modern fighters or even bombers. For example, Russia had stated that they are considering introducing an unmanned strategic bomber after 2040 whilst the USAF had explored optionally manned bombers in the Long-Range Strike Bomber programme.[18] Tactical fighters such as the F-16 had also been converted to unmanned versions as high-speed manoeuvrable target drones while the unmanned K-MAX helicopters demonstrated UAVs' versatility by taking up the cargo lift role in Afghanistan.[19] These examples prove the viability of UAVs in carrying similar payload as manned platforms.

Losses Due to Enemy Fire and Poor Reliability

UAVs are vulnerable to enemy fighters and air defence systems as they are usually not equipped with Electronic Countermeasures such as Chaff/Flare/Radar Warning Receivers that can be found on most tactical fighters. As such, UAVs have mostly been used in relatively benign airspace. Most of the UAV losses in the Afghanistan and Iraq wars were due to poor reliability and resulted in significant financial losses for countries such as the United Kingdom.[20] For USAF, the RQ-4 Global Hawk, MQ-1 Predator and MQ-9 Reaper had a combined 9.31 accidents for every 100,000 hours of flying; more than triple the USAF fleet-wide average of 3.03.[21] UAVs are currently not subjected to internationally-recognised aviation standards and are often designed with greater tolerance of risk, which directly impacts the reliability of the system. The International Civil Aviation Organisation had indicated that the first set of UAV airworthiness standards will only be in place in 2018, and they will include air traffic management and 'sense and avoid' requirements in 2020, paving the way for manned/unmanned airspace integration.[22] Until then, UAV design standards will continue to lag behind the mature standards developed over years of manned operations.

Vulnerability to Electronic and Cyber Attacks

Any assessment of a UAV's vulnerability will be incomplete without a discussion on the impact of an EW environment on its datalinks and Global Positioning System (GPS). UAVs are subjected to potential unauthorised access to their video feeds as exemplified by the leakage of unencrypted UAV footage to Iraqi insurgents in 2009.[23] Other common threats to UAVs are GPS spoofing and jamming attacks. Spoofing fools GPS receivers into tracking counterfeit GPS signals and allow the enemy to take control of the UAV while jamming disrupts the GPS signals on the receiver end and results in loss of control of the aircraft. In 2012, Raytheon UK claimed that North Korea performed GPS jamming operations on a Schiebel S-100 Camcopter UAV in South Korea, which resulted in an aircraft crash.[24] Ground Control Stations are also vulnerable to cyber attacks due to software security vulnerabilities, which led to DARPA's research into High-Assurance Cyber Military Systems.[25] While countermeasures such as anti-jamming devices, more advanced encryption and software 'hardening' are being developed to reduce susceptibility to these attacks, it is envisaged that counter-UAV technology developments such as control datalink jamming will ramp up in the future as more military forces recognise the potential threats posed by UAVs.

Political Considerations

Despite the proliferation of UAVs in both military and civil sectors, there is still a growing stigma among the public of their usage, with their role in the CIA's hunter-killer missions leaving the deepest impression. Till date, only the US has openly admitted to the use of armed UAVs, with most countries either steering away from deployment of armed UAVs or choosing not to declare their usage due to political sensitivities. These sensitivities are illustrated by the limitations imposed by the Missile Technology Control Regime, the disarming of UAVs before they can be exported, and general public discourse.[26] As of now, most ASEAN military forces possess only Tactical UAVs which fulfil ISR roles. Notably, a number of nations in the region have embarked on indigenous UAV programmes such as Composites Technology Research Malaysia (CTRM) Aludra and Eagle and Indonesia's Wulung UAVs. Whilst the RSAF continues to acquire new UAV systems with more advanced electronics and capabilities, it should be aware of the potential of an UAV arms race in the region, as rapid UAV developments in China, Russia, and Israel will likely result in aggressive marketing to Association of Southeast Asian Nations (ASEAN) military forces, which are increasingly looking outward for technology transfer opportunities and advanced systems for force modernisation efforts. Singapore should also continue to develop indigenous UAV technologies through Defence Science Organisation (DSO) to maintain a technological edge over potential adversaries and nurture our local industries for future growth.

CONCLUSION

UAVs will definitely play an increasing role in the projection of airpower in the coming years. The advantages associated with UAVs, such as persistence, autonomy, low unit cost, flexible design and the removal of human lives from danger will continue to position UAVs as the go-to solutions for many future airpower challenges. However, civil airspace integration, frequency spectrum management, reliability, political sensitivities, integration challenges and vulnerability to electronic attacks continue to restrict the widespread use of UAVs across the entire spectrum of air operations. In the near future, manned platforms will continue to play an important role in airpower while UAVs will continue to take up 'dull, dirty and dangerous' tasks such as ISR over enemy airspace. However, it is envisaged that UAVs will eventually take over manned platforms in the second half of this century when the technologies for UCAVs, unmanned strategic bombers and even unmanned helicopters and tanker/transport are expected to mature. It is also projected that the corresponding network infrastructure and regulatory civil and military framework will eventually be as established and well-maintained as that of manned platforms. This future is dependent on the willingness of military forces and political governments to expand the roles of UAVs which will in turn drive their research and development, leading to UAVs which will eventually match, and even surpass manned platforms in performance and efficiency.

BIBLIOGRAPHY

Carlo Kopp, "Western Complacency versus Growing SAM System Capabilities", Defence Today (March 2010): 32.

Carlo Kopp, "Surviving the Modern Integrated Air Defence System", Air Power Australia Analysis, 3 February 2009, http://www.ausairpower.net/APA-2009-02.html [Accessed 15 February 2015].

Gordon Arthur, "Taking Control – Asia-Pacific AEW&C Aircraft Programmes", Defence Review Asia, 6 June 2013, http://www.defencereviewasia.com/articles/221/TAKING-CONTROL-ASIA-PACIFIC-AEW-C-AIRCRAFT-PROGRAMMES [Accessed 15 February 2015].

James Hardy, "Indonesia, South Korea sign up for next phase of KFX programme", IHS Jane's Defence Weekly, 7 October 2014, http://www.janes.com/article/44212/indonesia-south-korea-sign-up-for-next-phase-of-kfx-programme [Accessed 15 February 2015].

Miroslav Gyusori and Chris Pocock, "Counter-Stealth Technology Flourishes in Europe", Aviation International News, 13 July 2014, http://www.ainonline.com/aviation-news/defense/2014-07-13/counter-stealth-technology-flourishes-europe [Accessed 15 February 2015].

Felix K. Chang, "Comparative Southeast Asian Military Modernization – I", The ASAN Forum, 1 October 2014, http://www.theasanforum.org/comparative-southeast-asian-military-modernization-1/ [Accessed 15 February 2015].

Lynn E. Davis et al., "Armed and Dangerous? UAVs and U.S. Security", RAND Corporation, 1 May 2012, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR449/RAND_RR449.pdf [Accessed 16 February 2015].

Zachary Keck, "China to Sell Saudi Arabia Drones", The Diplomat, 8 May 2014, http://thediplomat.com/2014/05/china-to-sell-saudi-arabia-drones/ [Accessed 16 February 2015].

"Iran Suicide Drone Tested During Military Exercise", CBCNews, 27 December 2014, http://www.cbc.ca/news/world/iran-suicide-drone-tested-during-military-exercises-1.2884674 [Accessed 16 February 2015].

Sydney J. Freedberg Jr., "X-47B Drone & Manned F-18 Take Off & Land Together in Historic Test", Breaking Defense, 17 August 2014, http://breakingdefense.com/2014/08/x-47b-drone-manned-f-18-take-off-land-together-in-historic-test/ [Accessed 16 February 2015].

Dan Parsons, "NASA Launches Study for Skunk Works SR-72 Concept", Flightglobal, 17 Dec 2014, http://www.flightglobal.com/news/articles/nasa-launches-study-for-skunk-works-sr-72-concept-407222/ [Accessed 17 February 2015].

Marina Malenic, "USAF Declares Gorgon Stare Follow-on Operationally Deployable", IHS Jane's Defence Weekly, 2 July 2014, http://www.janes.com/article/40290/usaf-declares-gorgon-stare-follow-on-operationally-deployable [Accessed 17 February 2015].

"Mind's Eye Surveillance to Watch, Identify and Predict Human Behavior from Video", Network World, 29 October 2012, http://www.networkworld.com/article/2223400/microsoft-subnet/mind-s-eye-surveillance-to-watch--identify-and-predict-human-behavior-from-video.html [Accessed 17 February 2015].

Wendell Minnick, "China's Checkmate: S-400 Looms Large Over Taiwan", Defense News, 7 December 2014, http://www.defensenews.com/story/defense/international/asia-pacific/2014/12/06/chinas-checkmate-s-400-looms-large-over-taiwan/20000373/ [Accessed 17 February 2015].

Dave Majumdar, "Russia Considering Unmanned Strategic Bomber for Deployment in the 2040s", Flightglobal, 28 August 2012, http://www.flightglobal.com/blogs/the-dewline/2012/08/russia-considering-unmanned-st/ [Accessed 18 February 2015].

Aaron Mehta, "Bomber Leads way on USAF RDT&E Request", Defense News, 2 February 2015, http://www.defensenews.com/story/defense/policy-budget/budget/2015/02/02/bomber-leads-way-on-usaf-rdte-request/22749943/ [Accessed 18 February 2015].

Marina Malenic, "K-MAX Ends Afghanistan Deployment, USMC Studies Data", IHS Jane's Defence Weekly, 24 July 2014, http://www.janes.com/article/41190/k-max-ends-afghanistan-deployment-usmc-studies-data [Accessed 18 February 2015].

Nick Hopkins, "Nearly 450 British Military Drones Lost in Iraq and Afghanistan", The Guardian, 12 February 2013, http://www.theguardian.com/uk/2013/feb/12/450-british-military-drones-lost [Accessed 20 February 2015].

Brendan McGarry, "Drones Most Accident-Prone U.S. Air Force Craft: BGOV Barometer", Bloomberg Business, 18 June 2012, http://www.bloomberg.com/news/articles/2012-06-18/drones-most-accident-prone-u-s-air-force-craft-bgov-barometer [Accessed 20 February 2015].

Bill Carey, "ICAO Panel Will Recommend First UAV Standards in 2018", Aviation International News, 6 January 2015, https://www.ainonline.com/aviation-news/aerospace/2015-01-06/icao-panel-will-recommend-first-uav-standards-2018 [Accessed 20 February 2015].

Mike Mount and Elaine Quijano, "Iraqi Insurgents Hacked Predator Drone Feeds, U.S. Official Indicates", CNN, 18 December 2009, http://edition.cnn.com/2009/US/12/17/drone.video.hacked/ [Accessed 20 February 2015].

Chris Pocock, "UAV Crash in Korea Linked to GPS Jamming", Aviation International News, 1 June 2012, http://www.ainonline.com/aviation-news/defense/2012-06-01/uav-crash-korea-linked-gps-jamming [Accessed 20 February 2015].

Jaikumar Vijayan, "DARPA Unveils Hack-Proof Drone Tech", Computerworld, 27 May 2014, http://www.computerworld.com/article/2489864/vertical-it/darpa-unveils-hack-proof-drone-tech.html [Accessed 20 February 2015].

Chris Pocock, "Predator UAV Cleared for Wider Export", Aviation International News, 4 March 2011, http://www.ainonline.com/aviation-news/defense/2011-03-04/predator-uav-cleared-wider-export [Accessed 20 February 2015].

Paul Harris, "Anti-drones Activists Plan Month of Protest Over Obama's 'Kill' Policy", The Guardian, 27 March 2013, http://www.theguardian.com/world/2013/mar/27/anti-drone-activists-protest-obama [Accessed 20 February 2015].

ENDNOTES

1. Carlo Kopp, “Western Complacency versus Growing SAM System Capabilities”, Defence Today (March 2010): 32.

   Carlo Kopp, “Surviving the Modern Integrated Air Defence System”, Air Power Australia Analysis, 3 February 2009, http://www.ausairpower.net/APA-2009-02.html.

   Gordon Arthur, “Taking Control – Asia-Pacific AEW&C Aircraft Programmes”, Defence Review Asia, 6 June 2013, http://www.defencereviewasia.com/articles/221/TAKING-CONTROL-ASIA-PACIFIC-AEW-C-AIRCRAFT-PROGRAMMES.

   James Hardy, “Indonesia, South Korea sign up for next phase of KFX programme”, IHS Jane’s Defence Weekly, 7 October 2014, http://www.janes.com/article/44212/indonesia-south-korea-sign-up-for-next-phase-of-kfx-programme.

2. Miroslav Gyusori and Chris Pocock, “Counter-Stealth Technology Flourishes in Europe”, Aviation International News, 13 July 2014, http://www.ainonline.com/aviation-news/defense/2014-07-13/counter-stealth-technology-flourishes-europe.

3. Felix K. Chang, “Comparative Southeast Asian Military Modernization – I”, The ASAN Forum, 1 October 2014, http://www.theasanforum.org/comparative-southeast-asian-military-modernization-1/.

4. Non-kinetic weapons, as defined by the USAF Doctrine Document 2, refers to logical, electromagnetic, or behavioural actions, such as a computer network attack on an enemy system or a psychological operation aimed at enemy troops. The effects they impose are mainly indirect.

5. The first remotely piloted drone used as a weapon was the German FX-1400, which consisted of a 2,300 pound bomb, dropped from an airplane and steered by a pilot in the main aircraft. It was deployed during World War II.

6. Initial testing of missile-equipped drones was completed in 2001, soon after the September 11 attacks the weaponised Predator UAVs, armed with Hellfire missiles, were flying over Afghanistan for the US invasion. In OEF alone, there were a total of 1,160 weapons released from armed UAVs, out of a total of 3,600 weapons released, showing the increasing role of UAVs for close air support missions.

7. Lynn E. Davis et al., “Armed and Dangerous? UAVs and U.S. Security”, RAND Corporation, 1 May 2012, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR449/RAND_RR449.pdf.

8. Ibid.

9. Zachary Keck, “China to Sell Saudi Arabia Drones”, The Diplomat, 8 May 2014, http://thediplomat.com/2014/05/china-to-sell-saudi-arabia-drones/.

10. “Iran Suicide Drone Tested During Military Exercise”, CBCNews, 27 December 2014, http://www.cbc.ca/news/world/iran-suicide-drone-tested-during-military-exercises-1.2884674

11. Sydney J. Freedberg Jr., “X-47B Drone & Manned F-18 Take Off & Land Together in Historic Test”, Breaking Defense, 17 August 2014, http://breakingdefense.com/2014/08/x-47b-drone-manned-f-18-take-off-land-together-in-historic-test/.

12. UAVs are typically designed to be smaller as compared to manned platforms due to the absence of a cockpit, ejection seat and bulky environmental control systems to regulate the pressure and oxygen levels required for the pilot. This allows the UAV design to be more flexible to reduce radar cross-section.

13. NASA has awarded a contract to Lockheed Martin to study into an unmanned, reusable hypersonic ISR and strike aircraft capable of Mach 6.0 flight.

    Dan Parsons, “NASA Launches Study for Skunk Works SR-72 Concept”, Flightglobal, 17 Dec 2014, http://www.flightglobal.com/news/articles/nasa-launches-study-for-skunk-works-sr-72-concept-407222/.

14. Marina Malenic, “USAF Declares Gorgon Stare Follow-on Operationally Deployable”, IHS Jane’s Defence Weekly, 2 July 2014, http://www.janes.com/article/40290/usaf-declares-gorgon-stare-follow-on-operationally-deployable.

15. “Mind’s Eye Surveillance to Watch, Identify and Predict Human Behavior from Video”, Network World, 29 October 2012, http://www.networkworld.com/article/2223400/microsoft-subnet/mind-s-eye-surveillance-to-watch--identify-and-predict-human-behavior-from-video.html.

16. Wendell Minnick, “China’s Checkmate: S-400 Looms Large Over Taiwan”, Defense News, 7 December 2014, http://www.defensenews.com/story/defense/international/asia-pacific/2014/12/06/chinas-checkmate-s-400-looms-large-over-taiwan/20000373/.

17. WVR engagements are defined as engagements with targets within the visual range of the pilot. BVR engagements are defined as engagements with targets beyond the visual range of the pilot, but are visible on radar or via other artificial means such as AWACs.

18. Dave Majumdar, "Russia Considering Unmanned Strategic Bomber for Deployment in the 2040s", Flightglobal, 28 August 2012, http://www.flightglobal.com/blogs/the-dewline/2012/08/russia-considering-unmanned-st/.

    Aaron Mehta, "Bomber Leads way on USAF RDT&E Request", Defense News, 2 February 2015, http://www.defensenews.com/story/defense/policy-budget/budget/2015/02/02/bomber-leads-way-on-usaf-rdte-request/22749943/.

19. Marina Malenic, "K-MAX Ends Afghanistan Deployment, USMC Studies Data", IHS Jane's Defence Weekly, 24 July 2014, http://www.janes.com/article/41190/k-max-ends-afghanistan-deployment-usmc-studies-data.

20. Nick Hopkins, "Nearly 450 British Military Drones Lost in Iraq and Afghanistan", The Guardian, 12 February 2013, http://www.theguardian.com/uk/2013/feb/12/450-british-military-drones-lost.

21. Brendan McGarry, "Drones Most Accident-Prone U.S. Air Force Craft: BGOV Barometer", Bloomberg Business, 18 June 2012, http://www.bloomberg.com/news/articles/2012-06-18/drones-most-accident-prone-u-s-air-force-craft-bgov-barometer.

22. Bill Carey, "ICAO Panel Will Recommend First UAV Standards in 2018", Aviation International News, 6 January 2015, https://www.ainonline.com/aviation-news/aerospace/2015-01-06/icao-panel-will-recommend-first-uav-standards-2018.

    Ibid.

23. Mike Mount and Elaine Quijano, "Iraqi Insurgents Hacked Predator Drone Feeds, U.S. Official Indicates", CNN, 18 December 2009, http://edition.cnn.com/2009/US/12/17/drone.video.hacked/.

24. Chris Pocock, "UAV Crash in Korea Linked to GPS Jamming", Aviation International News, 1 June 2012, http://www.ainonline.com/aviation-news/defense/2012-06-01/uav-crash-korea-linked-gps-jamming.

25. Jaikumar Vijayan, "DARPA Unveils Hack-Proof Drone Tech", Computerworld, 27 May 2014, http://www.computerworld.com/article/2489864/vertical-it/darpa-unveils-hack-proof-drone-tech.html.

26. The MTCR is an informal political understanding among states that seek to limit the proliferation of missiles and missile technology. It restricts export of rocket or UAV systems that are capable of delivering payloads of at least 500kg to a range of at least 300km.

    Chris Pocock, "Predator UAV Cleared for Wider Export", Aviation International News, 4 March 2011, http://www.ainonline.com/aviation-news/defense/2011-03-04/predator-uav-cleared-wider-export

    Paul Harris, "Anti-drones Activists Plan Month of Protest Over Obama's 'Kill' Policy", The Guardian, 27 March 2013, http://www.theguardian.com/world/2013/mar/27/anti-drone-activists-protest-obama.

ME4 Gerald Goh is an Air Force Engineer by vocation and is currently OC of Heron 1 IMF in 801 SQN. ME4 Gerald graduated from Imperial College London with a Masters of Engineering (Aeronautical Engineering).

FRAMEWORK FOR IDENTIFYING REQUIREMENTS IN THE DESIGN OF MULTI-DOMAIN COMMAND & CONTROL INFORMATION SYSTEM FOR TRI-SERVICE INTEGRATION

by ME5 Chua Zhongwang

Abstract:

This essay examines the challenges in designing a Command and Control Information System (CCIS) that shortens the Observe-Orientate-Decide-Act (OODA) cycle for an integrated Armed Force. This involves the co-ordination of air, land and sea assets of the Armed Forces, as well as cyber security necessary to ensure the robustness and resilience of the system. The mission-domains requirements of the CCIS and the impact of the environment and tactical operations at the different air-land-sea physical domains are examined in-depth. The essay also proposes a framework in the Requirement Analysis to achieve comprehensive requirements for CCIS system design across multi-domain operations.

Keywords: Command & Control; Communications; Information; Domain; Planning

INTRODUCTION

With the changing global landscape, the military's role has evolved from preparing and fighting the conventional war, to one that includes combating terrorism in counter-insurgencies operations, peace-keeping operations and Humanitarian Aid and Disaster Relief (HADR) operations. These operations often require the co-ordination of forces between different services in deploying air, land and sea assets in the Operational Theatre. To effectively command and control these forces, a common CCIS will be needed across the services to provide a Common Operating Picture (COP). In this essay, the author proposes a framework for identifying requirements in the design of such a CCIS system for different mission roles that spans across the air, land and sea domains, as well as in addressing the issue of cyber security to achieve a robust and resilient network with high capacity throughput.

IMPETUS

There is a rising trend of integrated operations where air, land and sea assets are employed in the same Operational Theatre to achieve mission success. Operation Desert Storm is an excellent example of this, where different assets from different services and nations are effectively deployed to achieve mission success in a short timeframe.[1] With this shift in operational focus, there is a strong impetus for the military to strengthen Command and Control of forces in different physical domains to enable a swift and decisive victory.

There is a rising trend of integrated operations where air, land and sea assets are employed in the same Operational Theatre to achieve mission success.

Achieving Information Superiority is another critical success factor in the modern battlefield. The military that is able to 'See First and See More' will gain significant advantages over the enemy and achieve mission success. This is best articulated in the article from Riscassi on the 4 key tenets to successful joint operations as stated below:[2]

1. Agility – Swift response and seize opportunities.
2. Initiative – Shorten OODA cycle and act first.
3. Depth – Pervasive awareness across entire spectrum of operations.
4. Synchronisation – Achieve common understanding and seamless operations outcome.

Another key aspect in the development of a robust and resilient CCIS system is in the area of cyber security.

An effective CCIS is identified as a key enabler to achieving the four tenets above. A well-designed CCIS will provide decision-makers with the COP for Pervasive Battlefield Awareness and decision-support algorithm for Superior Decision-Making.[3] When deployed to the frontline troops, the CCIS provides timely communications and effective task assignment to the different forces, preventing fratricide and enabling time-sensitive targeting.

LITERATURE RESEARCH

Timely, accurate and secured information form the basis for decision-making and is critical for the overall success of any military operations. In the article *'Air Force Aerial Layer Networking Transformation Initiatives'*, the authors highlighted the need for enhanced connectivity and collaboration as the top force multipliers.[4] In addition, the authors emphasised that multi-Service missions with dynamic operations will be more common resulting in an exponential rise in information nodes due to the increasingly complex and demanding operational environment. As a result, there is a greater need for higher bandwidth and automated decision support systems in the design of a CCIS.

These similar points are also articulated in the paper *'Army CCIS Requirements Definition'*.[5] Specifically, the author identified particular problems in the development of the land-based CCIS for the Army. These include constraints imposed by the environment and the large number of units in theatre (relative to other services) that the Army commands.

In the Navy, similar arguments can be found. In particular, the challenges for CCIS design in naval communications are expressed in the article, *'U.S. Navy Mass Communications Options*.'[6] Here, the authors focused on the uniqueness of naval operations far from land and without networking infrastructure. As a result, there is a particular need for the navy to invest in developing robust communications based on Beyond-Line-Of-Sight (BLOS) technologies.

Another key aspect in the development of a robust and resilient CCIS system is in the area of cyber security. With the CCIS being a highly networked system-of-systems, any cyber attack on the CCIS will result in crippling effects on the overall sense-making and decision-making capabilities of the military. In his article 'Cyber Threat – A Global Security Threat', the author highlighted a possible cyber defence framework to protect, detect and respond to cyber threats.[7]

BROAD REQUIREMENTS FOR TRI-SERVICE CCIS IN DIFFERENT MISSION-DOMAINS

The CCIS fulfils three key missions during military operations — 1) Strategic Planning, 2) Operational Control, and 3) Tactical Communications. As such, the functional Operational Requirements in the development of a joint CCIS must satisfy the operational needs that are unique to each of the three mission-domains. Here, a framework is proposed to elicit broad functional Operational Requirements that effectively and comprehensively defines the CCIS:

1. Strategic Planning. The CCIS is utilised by Senior Commanders to sense-make the current progress of the war-campaign. To fulfil this requirement, the CCIS must be able to maintain overall situation awareness of the friendly forces and potential enemy threats. The CCIS must have the flexibility to provide Senior Commanders with different Situation Pictures, from overall force deployment plans to logistics support plans and be equipped with Decision Support logic for large force employment planning. The CCIS will need to have the bandwidth and reach for the Senior Commanders to command and control the Operational Units in theatre, as well as information aggregation for effective decision-making. With up-to-date common situation pictures, the Senior Commanders will be better equipped to analyse and predict enemy's course of actions, and more effectively deploy own forces to achieve success in the overall campaign.

2. Operational Control. At the operational level, there is a need for Commanders to co-ordinate and control their forces in achieving each mission. Here, the CCIS will need to track positions of all friendly forces and enemy threats with a higher resolution and faster refresh rate, for effective control of the troops and assets in the theatre. In addition, the CCIS network will need to be pervasive and resilient to

2WO Sathiaseelan operating the Software Defined Radio (SDR) mounted on an Operations Utility Vehicle.

enemy's actions, such as jamming or spoofing, which will render the system ineffective for operations. With information received from the tactical-level units through the CCIS systems, the Operational Headquarters (HQ) will able to achieve pervasive battlefield awareness and execute superior decision-making to deploy resources to maintain an edge over the enemy. This capability will provide a Commander with dynamic operational control of his unit, enabling real-time tasking and re-role. For example, a fighter on a Precision-strike mission can be effectively deployed to provide Close Air Support (CAS) for ground troops that are under enemy attacks.

3. Tactical Communication. The CCIS will be deployed to the troops and assets (such as aircraft, tanks and Navy vessels) on the frontline who will be executing the mission. Here, the CCIS is required to provide timely and accurate updates to the troops with information such as friendly forces' and enemy forces' locations. As the troops are executing the missions and maneuvers, the CCIS must have a high refresh rate for timely updates and high resolution to discern between friendly and enemy forces. With the integration of the CCIS and remote sensors (such as radar), the troops will have real time tracking for friendly and hostile forces, enabling effective tactical operations while preventing fratricides. For example, with CCIS connectivity, the ground forces will be able to call in air-support with detailed position marking.

BROAD REQUIREMENT OF CCIS IN DIFFERENT PHYSICAL-DOMAINS

In addition to the requirements arising from the different mission domains of CCIS, the CCIS design is also greatly influenced by environmental factors for tactical operations in the different air-land-sea domains and the requirement for interconnectivity between them. As the key information highway, the CCIS must also be strengthened in the area of cyber security. In this regard, the challenges and requirements in the 4 different domains are indicated in the following paragraphs.

Air Domain

In the air domain, the air assets, mainly aircraft, are moving at a much higher speed as compared to the land and sea forces. As such, for effective sense-making, there is a need for the system to maintain a high refresh rate, especially at the tactical level. In addition, air assets typically operate at a greater distance from the Operational HQ as compared to land forces and there is a need for airborne CCIS to achieve greater range to account for distance and altitude. This is further coupled by the fact that relays may not be readily set-up in the air if there are no airborne command and control assets available. As such, air-borne CCIS will need to achieve high bandwidth with strong signal transmission and reception.

In addition, the modern fighter aircrafts are designed to be sleek and compact and are capable of high altitude and high-G maneuvers. As a result of the aircraft design, there are often size constraints for airborne CCIS equipment. The equipment must also be designed to meet operational specifications at high altitude and high stress environment due to G-loading.

Land Domain

In the land domain, the troops may be equipped with man-portable size CCIS equipment for information-gathering. With the man-portable remote sensors, the troops can track the positions of friendly and enemy forces to effectively engage hostility and allow the troops to navigate accurately through the terrain and avoid known danger areas. In addition, as the land

Minister for Defence, Dr Ng Eng Hen (left,) and Mrs Ng being briefed by Lieutenant Colonel Chew Chun-Chau, Head of RSN's LMV Project Office, during a tour of the ship's Integrated Command Centre.

forces fight in different unit sizes, from a Squad of special forces, to company-size and battalion-size attack forces, as well as tanks and other armoured vehicles, there is a need for customisation in CCIS equipping for the different forces.[8] For example, a Company Commander will need access to more information as compared to the Squad Commander; and a tank can have larger equipment with larger range that can function as a relay, as compared to the man-portable set.

In addition to the requirements arising from the different mission domains of CCIS, the CCIS design is also greatly influenced by environmental factors for tactical operations in the different air-land-sea domains and the requirement for interconnectivity between them.

One key environmental factor in the development of land-based CCIS equipment is the issue of line-of-sight (LOS). For example, connectivity of CCIS can be easily degraded by the lack of LOS in the dense forests in the tropics, or by buildings and enclosed environment in an urban setting, and the CCIS equipment must have the transmission and reception capabilities under such environmental constraints.

Another important factor for front-line tactical CCIS is ruggedness. Land operations, unlike air or sea, can take place under very different environmental conditions, such as torrential rains, dry hot deserts or in ice-cold winter. The equipment may also be subjected to rough handling and hard-knocks due to the nature of land operations. As such, the equipment must be designed to operate under these conditions.

Sea Domain

In the sea domain, the naval vessels may be deployed to open oceans far away from the mainland. As a result, there is a lack of communication network infrastructure or relay nodes between the naval vessels and the Operational HQ. Here, the key environmental challenge in the sea domain is in achieving sustained BLOS communications and options such as High-Frequency Radio, Military or Commercial Satellite communications will need to be considered for implementation.[9]

In addition to BLOS, the naval equipment will need to be designed for operations in sea-water conditions with high humidity and high salinity, as well as motions induced by sea waves. The resulting CCIS equipment for shipborne operations needs to be qualified and environmentally-tested differently from airborne or land equipment.

Cyber Security

The CCIS is a system-of-systems comprising different sensors and information nodes. This is achieved through a network of wired and wireless connections, using network and communication protocols. As such, the system, if not designed against cyber attacks, will be vulnerable to enemy actions. Here, the CCIS network will need to be protected against different kind of attacks, namely, 1) Information Gathering, 2) Information Denial and 3) Information Spoofing.

To address the issue of cyber security, the CCIS will be required to be designed with, 1) Message Security whereby messages are encrypted and protected to prevent information loss when messages are intercepted, 2) Transmission Security such as the use of Electronic Counter-Counter Measures (ECCM) techniques in waveform generation to prevent Jamming, and 3) Physical Security such as the use of Firewalls and physical safeguards in CCIS equipment.

FRAMEWORK FOR REQUIREMENT IDENTIFICATION

The proposed framework takes into account the mission-domain and physical-domain in which the CCIS will be operating, and identify categories of requirements applicable in system design.

Operational Role	Range of Coverage	Resolution of Systems	Redundancy of System	Physical Ruggedness	Refresh Rate
Strategic Planning	Long-Range (All forces across different countries).	Lowest – Aggregated Information at Divisional level.	Highly Redundant with fixed installation and backup systems.	Least as the equip is setup in protected Command Post	Lowest –Aggregated information and long term planning.
Operational Control	Mid-Range (All forces In-theatre).	Mid-range – Aggregated information at Squadron, or Flight level.	Mobile Setup with relative redundancy and backup of critical systems.	Mid-range as the setup may not be well-protected	Mid-range – Decision planning for immediate operations.
Tactical Comms	Short-Range (Forces at current mission).	Highest – resolution at individual and asset level.	Low Redundancy with backup provided by nearby friendly unit.	Highest as the equipment is exposed to the environment.	Highest – Report real-time changes for immediate actions and preventing fratricide.

Table 1: Mission-domain Related Requirements

	Environmental Effects	Operational Effects
Air	Altitude: - Design for transmission and bandwidth. - Hermetically sealed.	High-G Manoeuvre: - Ruggedness requirement. - G-tolerance requirement. Aircraft Size and Weight & Balance: - Limits physical dimensions and weight.
Land	Geographical: - Affecting Line-Of-Sight transmission (urban setting, forests). - Wide range of environmental condition (desert heat, cold winter). - Wide temperature range, and water-proofing requirements.	Decentralised C2: - Customisation for different users (Division Comd vs Company Comd vs Squad Leader). - Possible rough handling in a rugged environment.
Sea	Sea Environment: - High humidity and salinity. - Lateral motions induced by waves - Water-proofing Requirements - Ruggedness Requirements.	Far from Land: - Deploy far from fixed infrastructure. - Require robust Beyond-Line-Of-Sight communications.
Cyber	Pervasive across all deployed system: - Protect Against Information Gathering, Information Denial and Information Spoofing. - Message Security, Transmission Security, Physical Security Requirements.	

Table 2: Physical-Domain Related Requirement for Tactical Operations

In addition to requirements arising from the CCIS mission roles and physical-domains specific requirements, the CCIS will need to be designed with the following considerations:

1. ***Survivability.*** The CCIS shall maintain system integrity with a robust network such that there is no single point of failure—i.e. loss of individual nodes will not result in loss of entire network.

2. ***High Capacity.*** The CCIS shall be able to host and gather information from the respective units, using sub-networks as necessary to gather force-level information across different services and in different operational theatres.

3. ***Modularity.*** Due to the changing nature of today's operations, the CCIS shall be designed to be modular such that only necessary modules will be deployed in theatre. This is to enhance flexibility, while reducing deployment costs.

4. ***Decision Support.*** The CCIS provides an information rich environment for the decision-makers. However, this information glut may result in information overload, with delays in decision-making. To be effective, the CCIS shall be equipped with decision support algorithm to enable superior decision making.

5. ***Accuracy.*** Low Data Error Rate to ensure accuracy of transmitted information and tasking. In addition to effective communications, high accuracy will also strengthen the users' trust in the systems.

6. Reliability. The CCIS plays a critical role in today's military and a loss in CCIS capability may result in significant deterioration in the decision-making process. As such, the system shall be designed with a high reliability and availability. This, coupled with the redundancy in the system, shall provide the military with round-the-clock CCIS connectivity.

7. Maintainability. The CCIS equipment, especially equipment deployed to front line units, shall be highly maintainable to allow in-theatre repairs and servicing. For example, the systems shall be designed with low Mean-Time-To-Repair, and the maintenance tasks can be achieved using commonly-available tools.

8. Electro-Magnetic Interference/ Electro-Magnetic Compatibility (EMI/EMC). The tactical CCIS equipment will be deployed with the troops in operations. As a result, the equipment will be operating near explosives or ammunitions areas. As some of the CCIS equipment may have high power transmissions, CCIS equipment shall pass EMI/EMC testing prior to deployment for operational safety.[10]

9. Ease of Use. The CCIS must be user-friendly and allow users to operate the systems with minimal training. In addition, for tactical CCIS, the systems must be ergonomically-designed, especially in a high-tempo and high-stress operational environment.

10. Cost Effectiveness. Lastly, given the multitude of development and integration required in delivering the CCIS capability, Cost Effectiveness is a key consideration during the design process.

CONCLUSION

With a better understanding of the roles fulfilled by the CCIS and the environmental constraints affecting the tactical deployment of CCIS systems and equipment, the writer of this essay proposes a framework to identify requirements that are critical in the design of a tri-service CCIS. The writer feels that the framework will be useful during the Requirement Elicitation and Requirement Analysis phase of CCIS development to derive a baseline set of system requirements. It is important to recognise that the framework is not stagnant and will be enhanced as operational needs changes and new domains added. In this regard, further research can be conducted to include Space-Domain into the framework, and to expand scope in the Cyber domain.

ENDNOTES

1. P. Mason Carpenter, "Joint Operations in the Gulf War: An Allison Analysis". 1995.
2. Robert W. Riscassi, "Principles for Coalition Warfare," *Military Review*, v._ 73, n._ 6, 1993.
3. Singh, Ravinder; Tay, Andy; Ong, Melvyn; Lee, Jacqueline, *"IKC2 for the SAF: Organising around Knowledge"* POINTER, n._ 2, 12-18, 2007.
4. Schug, T.; Dee, C.; Harshman, N.; Merrell, R., "Air Force Aerial Layer Networking Transformation Initiatives," in Military Communications Conference, 2011, 1974-1978.
5. Kroening, Donald W., "Army Command and Control Information Systems Requirements Definition," *Systems, Man and Cybernetics, IEEE Transactions*, v._ 16, n._ 6, 974-979, 1986.
6. Breitler, A.L.; Nguyen, H.Q., "US Navy Mass Communications Options," Military Communications Conference, Conference Record, *IEEE*, v._ 3, 1093-1097, 1995.
7. Seah, S. T, "Cyber Threat – A Global Security Threat," *POINTER*, v._ 41, n._ 3, 51-63, 2015.
8. Ibid.

9. Ibid.

10. Eliardsson, P.; Axell, E.; Stenumgaard, P.; Wiklundh, K.; Johansson, B.; Asp, B., "Military HF communications considering unintentional platform-generated electromagnetic interference," in *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*, 1-6, 2015.

ME5 Chua Zhongwang was awarded the Academic Training Award and graduated from National University of Singapore in Mechanical Engineering (1st Class Honours). He also completed his dual Masters' degree under the Master of Defence Technology and Systems Programme, where he was the top student for the course. ME5 Chua is an Air Force Engineer by vocation and is currently Branch Head in Air Engineering and Logistics Department. His previous appointments include OIC in Air Logistics Squadron, Changi Air Base, OC in 5th Air Engineering and Logistics Group, and Staff Officer in HQ, Air Power Generation Command.

SOCIAL INTELLIGENCE AND MOTIVATION THEORIES IN TRANSFORMING THE RSAF

by CPT Varun Kumar Rai, LTA Benjamin Teng Yong Wei & LTA Dustin Jee Kam Chin

Abstract:

The working culture in the Republic of Singapore Air Force (RSAF) started out as a hierarchy culture, like most militaries. However, given the recent technological advances and shifts towards a more integrated and interdependent military, there has been a notable shift towards a somewhat clan culture. This essay aims to explain the shift in culture and its potential merits. It also aims to critically view the place that social intelligence has in this new culture and roles that different motivational theories may have on the individual. The authors also feel that an understanding of motivational theories would allow the RSAF to keep her people on the 'edge of their seat', maintaining a healthy balance between the two extremes of staying stagnant due to being unmotivated and complacent from too much motivation. The authors also feel that having a deep understanding of motivation would help build a cohesive and nurturing working environment for the RSAF.

Keywords: Social Intelligence; Motivation; Maslow's Hierarchy of Needs; Culture; Camaraderie

INTRODUCTION

The working culture in the RSAF started out as a hierarchy culture, like most militaries. This culture may have been a necessity in the past in order for the organisation to execute its wartime roles efficiently and effectively. However, given the recent technological advances and shifts towards a more integrated and interdependent military, there has been a notable shift towards a somewhat clan culture. Additionally, there has been an increasing focus and emphasis on engagement sessions between senior commanders and their men. This would not only help to foster the camaraderie within the unit but also help senior commanders better understand the needs of their men as well as help the men on the ground better understand the intent of senior commanders. This essay examines plausible reasons for this shift in culture as well as its potential merits. In particular, it focuses on how social intelligence is an important aspect of the clan culture as well as understanding motivational theories and their impact on the individual.

SOCIAL INTELLIGENCE

According to Kant, hard work alone cannot guarantee career success, and authors such as Riggio note that social intelligence is the key.[1] Hence, this section will break down the relevance and importance of social intelligence and its subset of emotional intelligence.

Kant explains that social intelligence is the equivalent of interpersonal intelligence, which is one of the intelligences identified in Gardner's Theory of Multiple Intelligences.[2] Shearer further breaks down interpersonal intelligence into two main skills.[3] The first skill is the ability to capture differences and distinguish individuals around them. In the Singapore

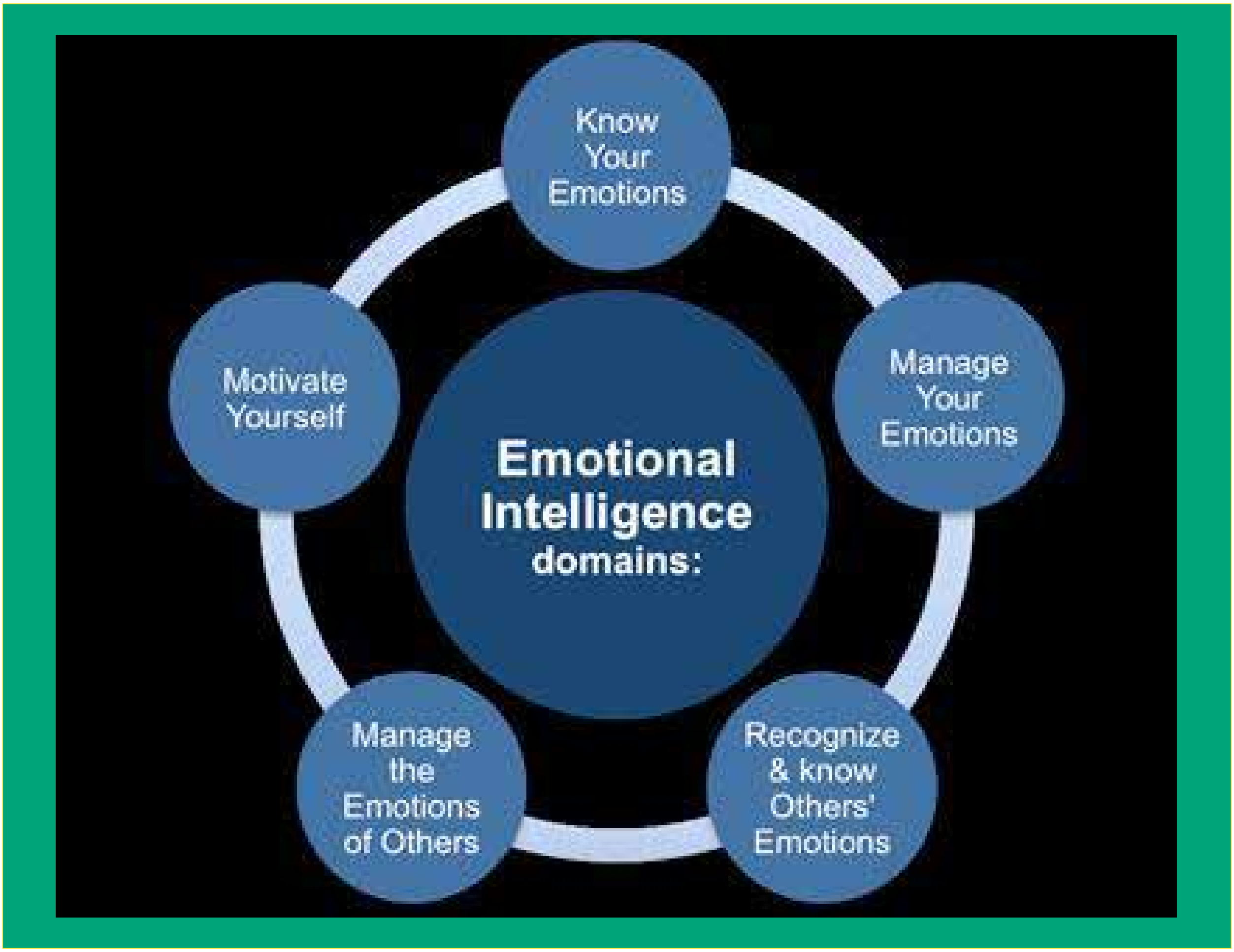

Know Your Emotions
Manage Your Emotions
Recognize & know Others' Emotions
Manage the Emotions of Others
Motivate Yourself
Emotional Intelligence domains:

Figure 1: Relationship between Self-Determination Theory (SDT) – Emotional Intelligence – Interpersonal Intelligence

Armed Forces (SAF), or in any organisation for that matter, such a skill is important for team leaders as it enables them to identify and capitalise on individual traits more efficiently and effectively. The second skill pointed out by Shearer is the ability to recognise emotions, perspectives and motivations of people.[4] Again, this is an important trait for commanders, teammates and subordinates as empathy could enhance the effectiveness of communication and ease of collaboration. Shearer further asserts that these social intelligence skills are critical factors in successful employment as they are associated with traits for leadership positions.[5] Hence, social intelligence skills are not only relevant to a clan culture, but are also important in achieving organisational excellence.

Another important observation is the correlation between social intelligence and self-motivation, which can be illustrated by a discussion on Emotional Intelligence (EI). Peter Salovey and John D. Mayer defined EI as a subset of social intelligence that involves the ability to not just recognise, but monitor the feelings and emotions of both oneself and others.[6] It also involves an ability to discriminate among them and more importantly, to use this information to guide one's thinking and actions. Goleman identified five domains of EI.[7] *Figure 1* shows how these domains encompass self-motivation and social intelligence.

To better illustrate how these theories can be practised in the RSAF as well as the benefits that can be gleaned from them, this essay uses the social intelligence model as defined by Karl Albrecht.

S.P.A.C.E. MODEL

Karl Albrecht profiled social intelligence into five broad categories which can be described by the SPACE acronym.[8] These five skillsets are: Situational Awareness, Presence, Authenticity, Clarity, and Empathy.

Situational Awareness is a pertinent skill set of social intelligence. It involves observing and understanding the environment that one is in. The epitome of the 3rd Generation RSAF is to be able to fight her battles as a system. To do so, situational awareness of each and every individual is critical for the RSAF to perform as a well-oiled machine.[9] Operators are equipped with a knowledge of their commander's intent on top of their primary objective. This allows them to look out for information that may fall outside of their mission and report intelligence that may reshape the battle.

The epitome of the 3rd Generation RSAF is to be able to fight her battles as a system. To do so, situational awareness of each and every individual is critical for the RSAF to perform as a well-oiled machine.

Presence is defined as the impression or image that you portray to others with respect to the way you behave. In the simplest form, it can be seen as 'bearing'. In the military, presence is very important and must not be neglected because a good presence will instil confidence to the public about you as well as the organisation. In the RSAF, the uniform we don is the simplest form of presence. It provides the soldiers with a sense of belonging as well as equality. More importantly, it is a form of identification for the public to know what profession we are in. Apart from 'bearing', the more important aspect of presence is one's behaviour and the mannerisms needed to create a good impression. Behavioural skills may be hard to develop and requires time. The RSAF has been actively finding ways to develop programmes such as SAF leadership competency models and the provision of Centre of Management and Development (CMD) courses to help servicemen to improve in this area. This helps the servicemen to portray a positive image of the RSAF to the public, which is an important aspect of organisational excellence.

Authenticity is basically the perception others may have of the congruence between one's ethical motives, behaviour and one's personal values. Having one mould for bosses and another for colleagues is not a sustainable long term endeavour that anyone can keep up with. Often times, this 'mould' cracks under pressure and results in a breach of trust either with one's superiors or colleagues. Given the demanding nature of military operations, being able to trust one's teammate is not only critical, it is imperative. Hence, the absence of such a trait may adversely affect one's ability to connect with the rest of one's peers. Additionally, authenticity is a key component in fostering genuine familial relationships, such as those in a clan culture.

Clarity involves the ability to express ideas across effectively and with impact. If presence defined the 'visual' aspect of social intelligence, Clarity will define the 'verbal' aspect. In RSAF as a whole, people come from diverse backgrounds with varying races, religions and educational levels. It is important to be aware of these diversities when communicating within the RSAF. In addition, clear communication is important in the RSAF because mistakes can be costly. Having clear communication is pivotal in preventing misinformation and confusion that may lead to accidents.

Empathy defined by Karl Albrecht is the ability to build meaningful connections with others.[10] He also defined that empathy is a notch higher by saying that feelings or connections have to be mutual between yourself and your partner. As the RSAF moves towards forging the tribe, it is important that servicemen understand how empathy can help forge meaningful relationships with one another. This in turn also creates a sense of belonging to the organisation and improves one's commitment to it.

MOTIVATION

The RSAF constantly operates in a dynamic and challenging environment. As a result, the RSAF has to constantly plan ahead to achieve a competitive advantage over her adversaries. In the RSAF, people play an important role in shaping policy planning and the future of Singapore's defence. Besides the importance of creating a nurturing and conducive working environment, it is also critical that the RSAF provides the right motivation for them to perform.

Motivation can be defined as what makes a person behave in a particular manner. The RSAF needs to constantly motivate their people, as it is an important and relevant driving force to achieve goal congruence. In general, motivation theories are categorised into content, process or psychological theories.

MASLOW'S HIERARCHY OF NEEDS (CONTENT THEORY)

Maslow's Hierarchy of Needs was established by Abraham Maslow as shown in *Figure 2*.[11] This theory explains the five human needs, which are ranked such that the lower, more basic needs must be satisfied before higher levels need to become activated. In the 3rd Generation transformation, the RSAF is able to activate and satisfy the higher level needs.[12] The RSAF has done considerably well in addressing the lower level needs with their competitive pay structure as compared to similar jobs in the private sector,

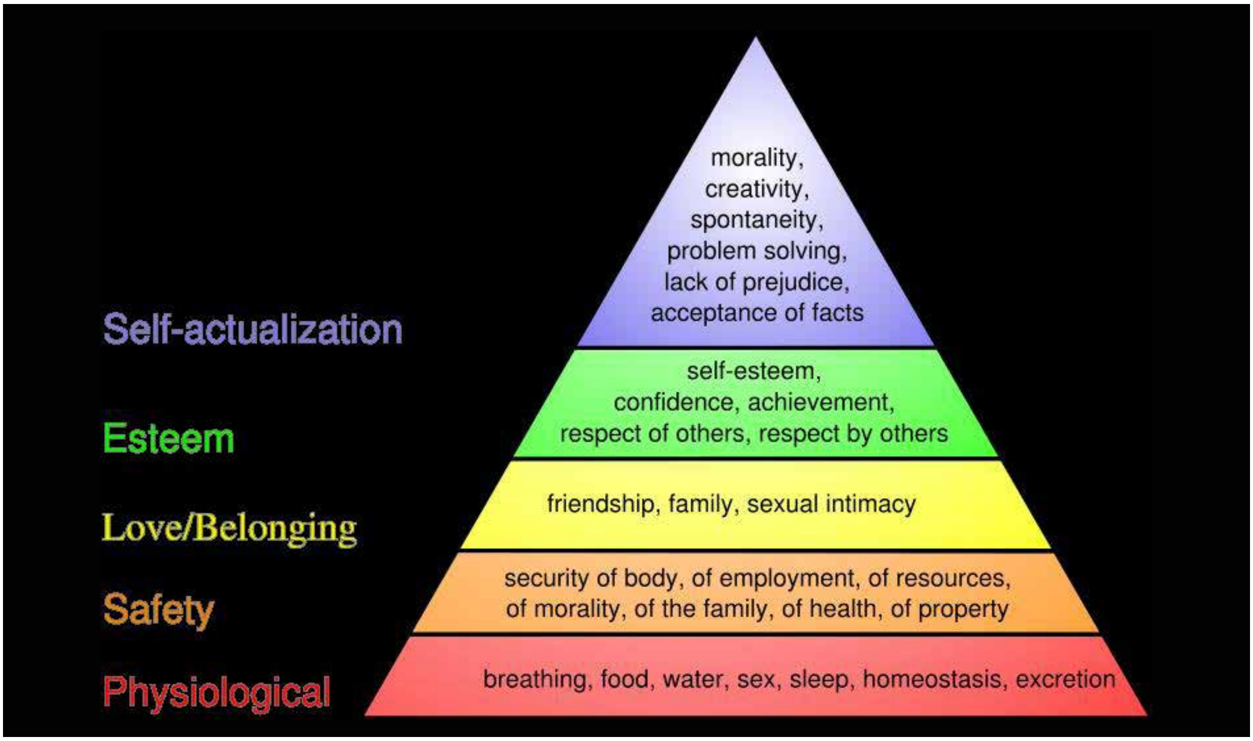

Self-actualization
morality,
creativity,
spontaneity,
problem solving,
lack of prejudice,
acceptance of facts
Esteem
self-esteem,
confidence, achievement,
respect of others, respect by others
Love/Belonging
friendship, family, sexual intimacy
Safety
security of body, of employment, of resources,
of morality, of the family, of health, of property
Physiological
breathing, food, water, sex, sleep, homeostasis, excretion

Figure 2: Maslow's Hierarchy of Needs

and also its excellent safety track record. In order to address the challenge of activating the higher level needs, the RSAF has introduced a People Development and Management framework called Project Cardinal. The framework hinges on three main pillars which are Developing Professionals, Realising Potential and Engaging the Heart. These three pillars are crucial to create a sense of belonging in their people and to satisfy their esteem needs.

The RSAF constantly operates in a dynamic and challenging environment. As a result, the RSAF has to constantly plan ahead to achieve a competitive advantage over her adversaries.

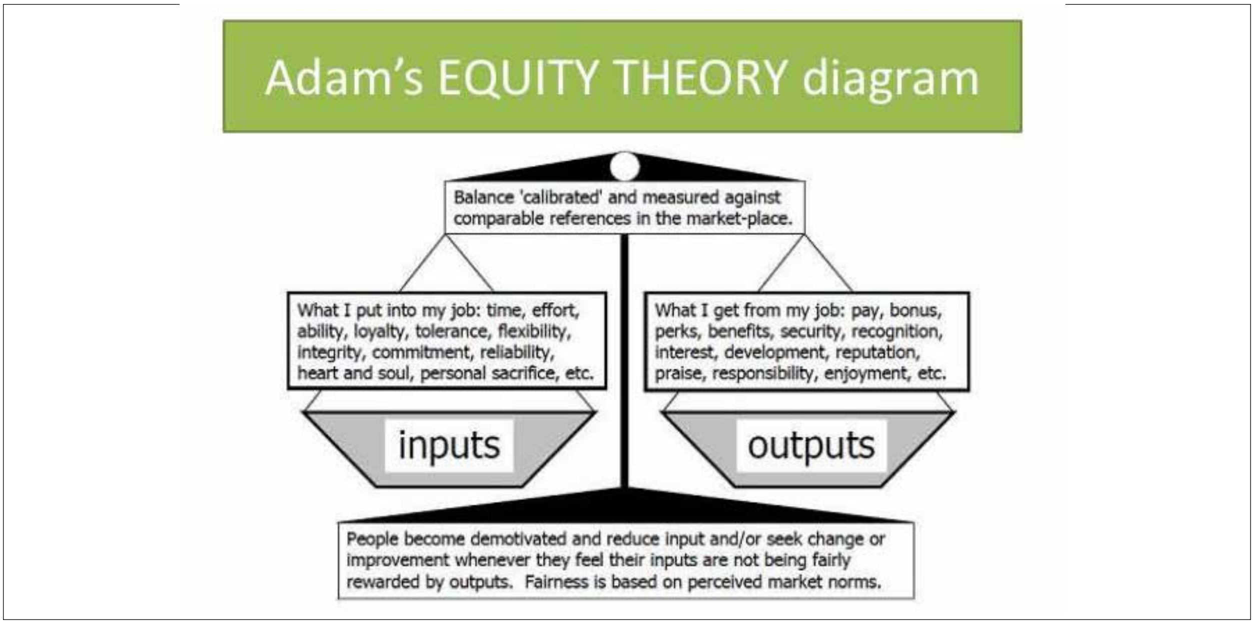
However, one important point to note from Maslow's theory is that a satisfied need may lose its motivational potential. Therefore, it is important for all levels of the organisation to constantly review, consolidate feedbacks and devise new programmes to satisfy their people's ever-changing needs.

ADAM'S EQUITY THEORY OF MOTIVATION (PROCESS THEORY)

Adam's Equity Theory of Motivation states that people will always strive for fairness and justice in social exchanges.[13] This means that people will be motivated only when their perceived inputs equal outputs to that of relevant others.

As depicted in *Figure 3*, a situation whereby the output is not equivalent to others can lead to either negative or positive inequity, both of which are not desirable to the organisation. For example, in the case of negative inequity, the employee feels undervalued because the effort put in does not commensurate with the rewards. This will likely result in the employee achieving equity by either reducing effort or increasing outcomes by demanding for higher rewards.

For positive inequity, the rewards are far greater than the amount of effort given. As a result, it is unlikely that employees will increase efforts or seek a lesser reward to achieve equity. In this case, the organisation stands to lose because of higher costs and not being able to motivate the employees to work at optimum.



Balance 'calibrated' and measured against comparable references in the market-place.

What I put into my job: time, effort, ability, loyalty, tolerance, flexibility, integrity, commitment, reliability, heart and soul, personal sacrifice, etc.

What I get from my job: pay, bonus, perks, benefits, security, recognition, interest, development, reputation, praise, responsibility, enjoyment, etc.

People become demotivated and reduce input and/or seek change or improvement whenever they feel their inputs are not being fairly rewarded by outputs. Fairness is based on perceived market norms.

Figure 3: Adam's Equity Theory of Motivation

A person's full potential can only be realised only if he or she is motivated. This theory highlights the importance of ensuring fairness and justice in the rewards system. For RSAF, these rewards can come in the form of annual ranking, performance bonus, job appointments, overseas posting opportunities, qualifications and many more. In general, the RSAF has a well-established system to give rewards and incentives. However, different people will have different perspectives on what is considered fair. It will be hard for the organisation to have a system to please everyone, as the system has to be robust, flexible and communicated to all levels of the organisations to ensure transparency. Studies have also shown that job performance and satisfaction are positively correlated to employee's perception of fairness in their organisation.

SELF-DETERMINATION THEORY (PSYCHOLOGICAL)

After evaluating the two motivation theories, we will now look at the psychological aspect of it. Self-Determination Theory (SDT) is explained by Deci and Ryan as a person's innate needs and the desire to seek growth in their lives.[14] There are two parts to SDT, which are a person's needs and motivation. SDT has identified three innate needs of people (Competence, Relatedness and Autonomy) as shown in *Figure 4*.

If these needs can be satisfied, an individual will be able to perform at an optimal level and experience growth. The RSAF has generally done well in tackling the psychological needs of people. The RSAF has robust training programmes such as the pilot training programmes where state-of-the-art simulators and aircrafts are used to train and hone the pilot's competencies. The RSAF also emphasises lifelong learning, for example through postgraduate scholarships, sponsorships and study awards.

One main pillar of Project Cardinal is to engage the hearts of the people. In the RSAF, there are mandatory cardinal activities organised across all levels of the organisations to instil a sense of belonging and relatedness to one another.

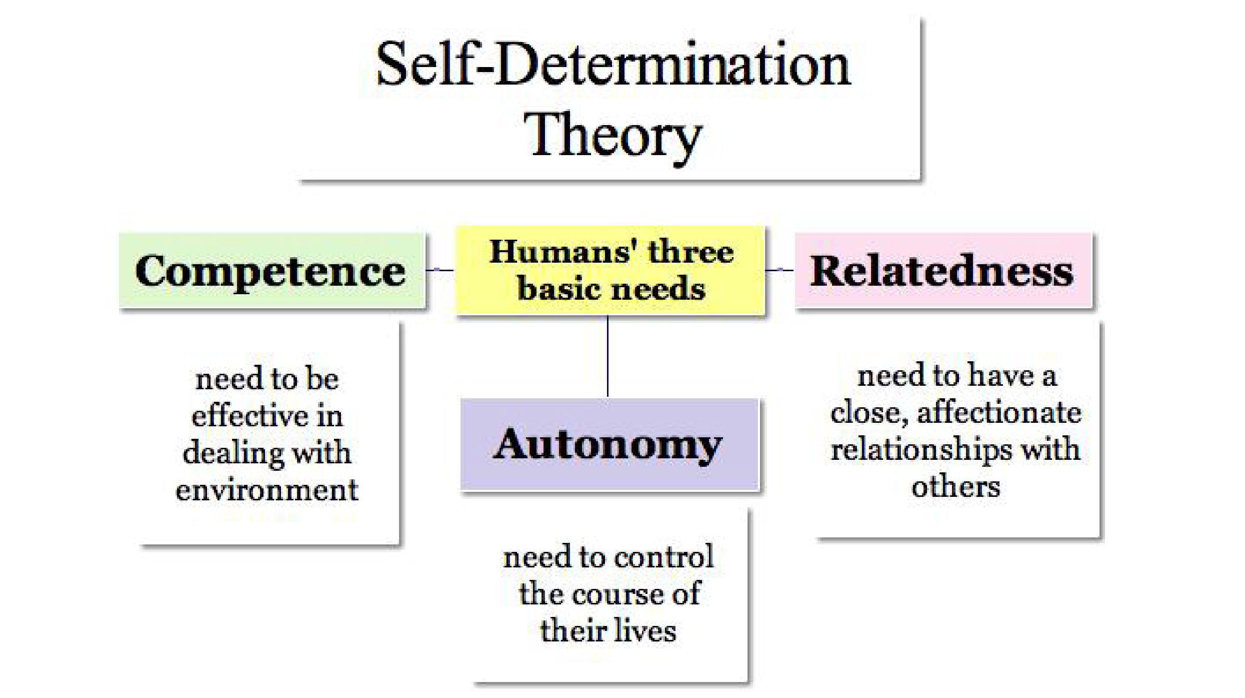

Self-Determination Theory
Competence
Humans' three basic needs
Relatedness
need to be effective in dealing with environment
Autonomy
need to have a close, affectionate relationships with others
need to control the course of their lives

Figure 4: Self-Determination Theory

Once the three needs are achieved, an individual will be intrinsically motivated to achieve their goals. Developing intrinsic motivation in an individual takes time and the RSAF has been taking a two-pronged approach in providing financial security as well as developing individuals.

Lastly, autonomy refers to the ability of a person to control and determine his own behaviour and goals. Autonomy is a very subjective subject in the RSAF as it is a military organisation. There are still rules and regulations to be followed as well as the hierarchical structure. However, the recent command restructuring into five commands has seen a more horizontal command hierarchy structure. This new structure has empowered greater autonomy through decentralisation to people on the ground, empowering them to make decisions that improve combat effectiveness. Autonomy is a crucial criterion for a person's development of self-determination, which in turn affects his motivation.[15] However, in giving autonomy, great care has to be given to ensure individuals do not abuse the freedom given to them.

Once the three needs are achieved, an individual will be intrinsically motivated to achieve their goals. Developing intrinsic motivation in an individual takes time and the RSAF has been taking a two-pronged approach in providing financial security as well as developing individuals. More importantly, research by Deci, Koestner and Ryan mentioned that having an extrinsic motivation may not be feasible in the long run as an individual may be led to 'detract from subsequent motivation.' This is also in congruence with Maslow's Hierarchy of Needs Theory, which asserts that as soon as a lower level need is satisfied, it loses its ability to motivate.[16]

CONCLUSION

In conclusion, we have seen how social intelligence and motivation theories have helped shaped RSAF policy towards organisational excellence. From research, it is deemed that social intelligence plays a major role in contributing to the organisation. The SPACE model by Albrecht, defined the important characteristics required for an organisation to function effectively.[17] Understanding of motivational theories allows the RSAF to keep her people on the 'edge of their seat', maintaining a healthy balance between the two extremes of staying stagnant due to being unmotivated and complacent from too much motivation.

Moving forward, the increasing integration of technology into the modern battlefield has greatly increased the complexity and pace of modern missions. Effective execution of the mission would require a deep understanding of each team member's strengths and weaknesses. On the peacetime front, having a deep understanding of motivation would help build a cohesive and nurturing working environment for the RSAF.

ENDNOTES

1. Kant, Kamal. Career Theories. In Work and Careers in the 21st Century. . Mc Graw Hill Education.

   "Intelligence Reframed: Multiple Intelligences for the 21st Century." Choice Reviews Online 37, no. 10 (2000).

2. Kant, Kamal. Career Theories. In Work and Careers in the 21st Century. . Mc Graw Hill Education.

3. Shearer, C. Branton. "Using a Multiple Intelligences Assessment to Promote Teacher Development and Student Achievement." Teachers College Record Teachers College Rec 106, no. 1 (2004): 147-62.

4. Shearer, C. Branton. "Using a Multiple Intelligences Assessment to Promote Teacher Development and Student Achievement." Teachers College Record Teachers College Rec 106, no. 1 (2004): 147-62.

5. Shearer, C. Branton. "Using a Multiple Intelligences Assessment to Promote Teacher Development and Student Achievement." Teachers College Record Teachers College Rec 106, no. 1 (2004): 147-62.

6. Salovey, Peter, and John D. Mayer. "Emotional Intelligence." Imagination, Cognition and Personality 9, no. 3 (1989): 185-211.

7. Goleman, Daniel. Emotional Intelligence. New York: Bantam Books, 1995.

   Goleman, Daniel. Emotional Intelligence. New York, NY: Bantam Books, 2006.

8. Albrecht, Karl. Social Intelligence: The New Science of Success. San Francisco: Jossey-Bass, A Wiley Imprint, 2006.

9. "POINTER - Journals - 2009 - Vol 35 No. 1 - The RSAF - Becoming a Full Spectrum, Integrated, and Ready Air Force." POINTER - Journals - 2009 - Vol 35 No. 1 - The RSAF - Becoming a Full Spectrum, Integrated, and Ready Air Force. Accessed February 22, 2016. http://www.mindef.gov.sg/imindef/publications/pointer/journals/2009/v35n1/feature1.html.

10. Albrecht, Karl. Social Intelligence: The New Science of Success. San Francisco: Jossey-Bass, A Wiley Imprint, 2006.

11. Maslow, A. H. "A Theory of Human Motivation." Psychological Review 50, no. 4 (1943): 370-96.

12. "CO07006 | The Transformation of the RSAF: The Organisational Dimension." CO07006. Accessed February 22, 2016. https://www.rsis.edu.sg/rsis-publication/idss/889-the-transformation-of-the-rsaf/#.VquFQFN97Uo.

13. Adams, J. Stacy. "Inequity In Social Exchange." Advances in Experimental Social Psychology, 1965, 267-99.

14. Deci, Edward L., and Richard M. Ryan. "Intrinsic Motivation and Self-Determination in Human Behavior." 1985.

15. Deci, Edward L., Richard Koestner, and Richard M. Ryan. "A Meta-analytic Review of Experiments Examining the Effects of Extrinsic Rewards on Intrinsic Motivation." Psychological Bulletin 125, no. 6 (1999): 627-68.

16. Maslow, A. H. "A Theory of Human Motivation." Psychological Review 50, no. 4 (1943): 370-96.

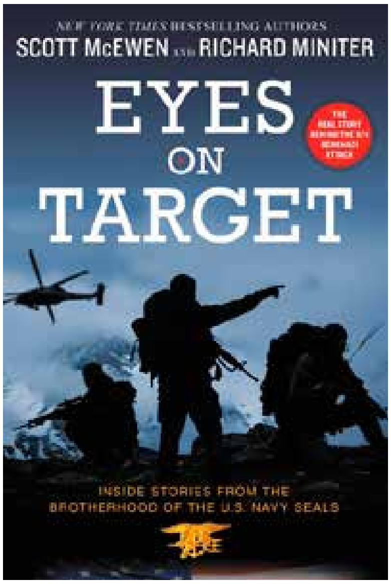
17. Albrecht, Karl. Social Intelligence: The New Science of Success. San Francisco: Jossey-Bass, A Wiley Imprint, 2006.

CPT Varun Kumar Rai is currently in 123 SQN. He graduated with a degree in Business (Banking & Finance)(1st Class Honours) from Nanyang Technological University (NTU). CPT Rai is a helicopter pilot by vocation.

LTA Benjamin Teng Yong Wei is currently an operational helicopter pilot in 125 SQN. He recently graduated from NTU with a Bachelors of Business (Honours).

LTA Dustin Kam Chin Jee is currently pursuing a degree in Economics from NTU. He is a Super Puma pilot by vocation, previously from 126 SQN.

Book Review


NEW YORK TIMES BESTSELLING AUTHORS
SCOTT McEWEN AND RICHARD MINITER
EYES ON TARGET
INSIDE STORIES FROM THE BROTHERHOOD OF THE U.S. NAVY SEALS

Scott McEwen and Richard Miniter, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs,* (New York, Center Street), 2014, 320 pages

By **Delson Ong**

INTRODUCTION

The United States (US) Navy's Sea, Air and Land Teams, commonly known as the Navy SEALs, are recognised worldwide as a reputable special operations force. It therefore comes as no surprise to find many books out there that document almost everything about them, from past to present. With that being said, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs* feels like a book that does not receive enough credit for the amazing stories that are documented.

The book contains accounts of major SEAL operations—from the Abbottabad raid to the Benghazi attack, just to name a few—all of which are presented in a chronological and concise manner. The authors touch on the background stories of several retired SEALs officers, all of whom contributed greatly to the history of one of the most feared fighting units in the world. Through this book, both Scott McEwen and Richard Miniter have pulled back the veil that has so often concealed the heroism of these patriots, and hope to change the reader's perception of the SEALs.

THE BROTHERHOOD

> *"The only thing that SEALs hate more than terrorists are 'fake SEALs'—civilians, or even other service members, who pretend to be a part of their sacred brotherhood."*[1]

Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs starts off with a small introductory chapter to provide readers with an understanding of the NAVY SEALs. Author Scott McEwen pens down his encounter of a SEAL impersonation incident that he witnessed firsthand, which illustrates clearly the fact that the brotherhood is scarily sacred, and for good reason. Because the road to becoming a SEAL (termed as 'evolution') is an arduous and daunting one, it is only right that the SEALs see the need to protect 'their own kind'. The SEAL Code and the SEAL Creed are also included in this introduction, albeit briefly, to cement the readers' understanding of the Navy SEALs.

ORIGINS OF THE NAVY SEALS

John Fitzgerald 'Jack' Kennedy, or more commonly known as John F. Kennedy, set in motion a lot of events during his stint as President of the United States (US). He is more widely known for the tax cuts that triggered the 1960s economic boom, as well as the developments in the Space Race to land the first men on the moon.[2] What is lesser known is that John F. Kennedy was integral in the creation of the US Navy SEALs as well. He imagined a mobile commando force that could stalk, hunt and kill in any terrain on earth, operating from ships, submarines and the aircrafts of the US Navy. Hence, in 1962 he signed off on the creation of a new type of frogman—the SEALs.

Drago

His true name is never revealed, as he remains under threat from terrorists. Nevertheless Drago's story illuminates a key chapter in the development of the SEALs. This book is the first to tell his tale (or most of it), to illustrate the openness of SEALs to new talents as Drago is a Polish immigrant, and he was much older than other men when he enlisted to join the SEALs.

The book covers much of Drago's childhood, even including his childhood story about a quarrel between his parents. This quarrel taught him one thing: Every obstacle can be overcome with persistence and creativity.[3] From young, he was a disobedient child, refusing to follow rules. His determination to get into the SEALs was beyond comprehension, something incredibly admirable about him. During his training to become a SEAL, Drago's leg was so swollen by flesh-eating bacteria that his shoe increased by a staggering three sizes, from a size ten to size thirteen and a half. Even that, however, could not stop him. When asked why he was so determined, these were his exact words:

> *"I did not come here to try to be a SEAL. I came here to become a SEAL. I did not come here to try, and I am not trying it. I am going to become a SEAL unless I get kicked out of training, or I break myself. I will become a SEAL."*[4]

His determination stunned everyone. In the missions that he undertook after becoming a full-fledged SEAL, Drago would find out that his unique history was constantly an unexpected asset in the SEALs. Although he was an immigrant, Drago says that he owes everything to America. For Drago, he did not believe in being Polish-American, or for that matter, being Something-American. You are either an American, or you are not. And I am an American.'[5]

OPERATION EAGLE CLAW

Readers are treated to a very vivid and detailed description of the timeline of events that took place. Operation Eagle Claw was an operation ordered by the US President at that time, Jimmy Carter, to attempt to end the Iran hostage crisis in Tehran, Iran's capital city.[6] Some 52 American diplomats and US Marines were taken hostage on 4th November, 1979 by an armed mob that had surged into the US embassy compound in Tehran.[7] The scheduled rescue plan took months to materialise, but eventually it was aborted due to various reasons.

The Mission That Was Not Meant To Be

Operation Eagle Claw was set to commence on 24th April, 1980, some five months after the American diplomats and US Marines were taken hostage. Although the crewmen that were involved were confident that their individual parts would work as expected, no one saw the big picture. Nothing they did could have prepared them for what happened on that fateful day.

Everything went as planned on the day itself, but shortly after they landed at Desert One (a desolate and uninhabited location located 200 miles from Tehran), their cover was blown. The element of surprise was gone, but that was just the start of a chain of unfortunate events that would befall the rescuers. Eight helicopters were deployed in this mission that required a minimum of six, and as luck would have it, engine failures took out two helicopters. A *haboob* (a dense dust storm that moves across the desert) further reduced the number to five. There existed no possibility that five choppers would suffice as the required minimum was six, especially when the most difficult portion of the mission was still ahead of them. However, the worst was yet to come. As they were departing, one helicopter moved in to one of the C-130s to refuel, but the chopper got too close for comfort and they collided into each other, setting off a fireball.[8]

SEAL TEAM SIX

The hostages were freed after 444 days of captivity, ending the Iran Hostage Crisis. Yes, the rescue mission was a failure in many ways, and the US Defence Department would spend months drawing hard lessons from this bitter tutorial. But the mission succeeded in one aspect: the failure of Operation Eagle Claw led to the creation of SEAL Team Six.

Richard Marcinko – Founder of Seal Team Six

In the wake of Operation Eagle Claw, founder of SEAL Team Six, Lieutenant Commander Richard Marcinko, was tasked with the design and development of a full-time dedicated counter-terrorist team. At that time, the Navy had only two SEAL teams, and Marcinko deliberately named the new unit SEAL Team Six, in an effort to trick others into thinking that the US had three other SEAL teams that they were unaware of.[9]

What was unique was the way that SEAL Team Six worked. It functioned very differently from other special task force units, almost as though they were part of a separate organisation. In SEAL Team Six, there exists a very unique culture, all thanks to Marcinko himself. Normally, we would expect Navy personnel to look like your typical military types, with tightly shaved hair and polished boots. However, the officers and the men of this special unit looked nothing like that. All of them sported beards, long hair, and even tattoos, making any normal-looking naval officer look like an oddball instead. The description of how SEAL Team Six looked like, in my opinion, was particularly well-written.

Neither did the typical military hierarchy exist in here—everything worked in reverse. In Team Six, senior enlisted men ran day-to-day operations, not the new guys. And despite having a higher rank, officers had to earn the respect of these men. In any other place in the Navy, men would salute the superiors. But in SEAL Team Six, it would be unwise for an officer to buck the senior enlisted men even if they were technically under him. To quote the author, SEAL Team Six seemed like a 'world turned upside down'.[10]

BATTLE OF BENGHAZI

Also known as the 2012 Benghazi Attack, the event took place on 11th September, 2012, where Islamic militants attacked the American diplomatic compound in Benghazi, Libya and killed US Ambassador Christopher Stevens.[11] Four chapters were dedicated to this significant event in American and Navy SEAL history The first two explained the event as it happened, and the third proposed several rescue scenarios that could have taken place. Amazingly, the fourth chapter consists of a detailed timeline of events of the Benghazi Attack, which was pieced together by the authors themselves.

There was no distinction, to the men in the various SEAL Teams, whether or not the people involved in the Battle of Benghazi were no longer active-duty SEALs when they had fallen. They were SEALs at one point in time, and they died trying to save American lives.[12] Many SEALs were angry with the President, and the entire chain of command, but this is not the only time that the SEALs would find their fellow team mates involved in tragedies that could have been prevented.

THE ESSENTIAL REALITY

In the crackle of radio static or a flash of text, team mates they have known for years—could suddenly be gone. This is the essential reality that every SEAL has to face, that death stalks them just as they bring it to their nation's enemies.[13]

Of the many special units that could be chosen to execute Osama bin Laden, the SEALs were sent in to bin Laden's lair. Although it has been a hot debate topic among special operators, one thing is for sure: being handpicked to visit America's number one enemy is a testament to the effective combat capability of the Navy SEALs. The bulk of the chapter on the bin Laden raid was cleverly written, whereby the authors broke up the SEAL creed into parts to show how the SEALs operate under pressure, where their actions are guided by the very principles hammered into them through years of discipline and thousands of man-hours of training.

Casual Use of Seal Teams Led To Tragedy

With bin Laden taken down, the heroic deeds of SEAL Team Six were trumpeted in the headlines of every major news organisation around the world. The glorification of their victory made them targets as well, and the SEALs knew it.

The aftermath of the raid was the biggest single loss of life in SEAL history. Three months after the raid, a helicopter was shot down by a rocket-propelled grenade in Afghanistan, killing all thirty-eight members on board, including 15 members of SEAL Team Six. Families of the victims and the public faulted the Obama administration for the casual use of SEAL Teams. Only two days after Osama bin Laden was killed, US Vice President Joe Biden's reckless comments violated the operational security needed for covert missions when he singled out SEAL Team Six as responsible for the death of bin Laden.

Although it is impossible to say with certainty that naming the executioners led to their deaths, there is no doubt that the Obama administration's actions broke the trust between the SEALs and the president. In my opinion, there certainly is a pride in being a SEAL. However, therein lies the problem as well—one can never be too easy in letting others in on what they do.

CONCLUSION

Credit has to be given to the authors for the way the book is written. Despite having to document many operations involving the Navy SEALs. There are indeed many books on the Navy SEALs, but this book is the first of its kind that treats them as characters in their own right. There are many other operations and characters not mentioned here, but they are definitely worth reading up on as well. For aspiring readers who are interested to find out more about the Navy SEALs, this is the book to start with.

ENDNOTES

1. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), ix.
2. Ibid., 6.
3. Ibid., 57.
4. Ibid., 63.
5. Ibid., 69.
6. *Operation Eagle Claw*, (Wikipedia) https://en.wikipedia.org/wiki/Operation_Eagle_Claw

7. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 20.

8. Ibid., 37.

9. *Richard Marcinko*, (Wikipedia) https://en.wikipedia.org/wiki/Richard_Marcinko

10. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs,* (New York, Center Street, 2014), 46.

11. *2012 Benghazi Attack*, (Wikipedia) https://en.wikipedia.org/wiki/2012_Benghazi_attack

12. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs,* (New York, Center Street, 2014), 142.

13. Ibid., 191.

William Joseph Donovan (1883-1959)

by **Macalino Minjoot**

INTRODUCTION

William Donovan was a well decorated soldier, lawyer, intelligence officer and diplomat of the United States (US) and was the only person to receive all four of the highest awards in the US: The Medal of Honour, the Distinguished Service Cross, the Distinguished Service Medal, and the National Security Medal.[1] These medals are a testimony to the amount of work and effort William Donovan has put in for his country.

EARLY LIFE

William Joseph Donovan was born on 1st January, 1883, in Buffalo, New York. His father and mother, Timothy P. Donovan and Anna Letitia 'Tish' Donovan respectively, were first generation immigrants of Irish descent. There were originally nine children, but four died of spinal meningitis at an early age.[2]

William Donovan attended St. Joseph's Collegiate Institute and Niagara University before transferring to Columbia University to study Law. William Donovan was very athletic and on the football field he was nicknamed 'Will Bill'—a nickname that would remain with him for the rest of his life. Other than being athletic, his other extra-curricular activity was debating, for which he won the George William Curtis Medal for Public Speaking. One of William Donovan's classmates at law school was Franklin Delano Roosevelt, but they were in different social circles and were not well acquainted until Roosevelt became president. In 1905, William Donovan graduated from the Columbia Law School and then became an influential Wall Street lawyer.

In May 1912, William Donovan was keen to serve his country—he formed a troop of cavalry of the New York National Guard and the unit was designated Troop I, 1st New York Cavalry. In October, Donovan was elected captain of the troop and his unit was mobilised in 1916 and served on the US-Mexico border during the American government's campaign against Pancho Villa.[3]

WORLD WAR I

During World War I (WWI), Donovan served his country again, when his regiment, the popular 69th, was called into federal service. During his time leading the 1st battalion of the 165th Regiment of the 42nd Division, which were the federalised designation of the popular 69th New York Volunteers (also as known as 'Fighting 69th'), Donovan once again earned his nickname 'Wild Bill'.[4] The men in his battalion called him 'Wild Bill' out of admiration for his calm and resourcefulness during combat and because of the hard physical drills he made them do to prepare for battle.

Donovan was wounded in action three times during WWI. On 18th July, 1918, for bravery under fire on the River Ourcq during the Second Battle of the Marne, he was awarded the Medal of Honour. By the end of the war, Donovan had been promoted to colonel and was one of the most decorated soldiers of WWI. Upon returning from Europe after World War I, Donovan - along with Theodore Roosevelt, Jr. - was a co-founder of the American Legion.[5]

BETWEEN THE WARS

From 1922 to 1924 after WWI, there were a number of threats to assassinate Donovan and to dynamite his home but he was not deterred as he was the US Attorney for the Western District of New York, famous for his energetic enforcement of Prohibition in the US. He believed that the law should be upheld impartially and aroused great indignation. At one time, large amounts of illegal liquor were confiscated when his agents raided an upmarket, Saturn Club, on Delanware Avenue. As Donovan was a member of the upmarket, some members assumed that the Prohibition in the US did not apply to them. When the illegal liquor was confiscated, some of the upmarket members felt that Donovan was a traitor to his class.

Donovan ran unsuccessfully as a Republican for Lieutenant Governor of New York in 1922, and for Governor of New York in 1932. Assisting Donovan in his 1932 campaign was journalist James J. Montague, who served as a 'personal adviser and campaign critic.'[6]

WORLD WAR II

During the interwar years, Donovan travelled extensively in Europe and met with foreign leaders including Benito Mussolini of Italy. Donovan openly believed during this time that a second major European war was inevitable. His foreign experience and realism earned him the attention and friendship of President Franklin D. Roosevelt. The two men were from opposing political parties, but were similar in personality. During these trips, Donovan met with key officials in the British war effort, including Winston Churchill and the directors of Britain's intelligence services. Donovan returned to the US confident of the possibility of founding an American intelligence service modelled on that of the British.

Office of Strategic Services

On 11th July, 1941, Donovan was named Co-ordinator of Information (COI). America's foreign intelligence organisations at the time were fragmented and isolated from each other. The Army, Navy, Federal Bureau of Investigation (FBI), United States Department of State and other departments each ran its own intelligence operations, the result of which was that they were reluctant to share with one another. Donovan was the nominal director and had plans of a merger to share information but the leaders were not willing to give up their power within the current separate services. The FBI, in particular, was under the control of J. Edgar Hoover (Donovan's rival). Hoover insisted on retaining its target and focus on South America.

Nevertheless, Donovan started to lay the groundwork for a centralised intelligence programme. He organised the COI's New York headquarters at Rockefeller Centre and asked Allen Dulles to head it, the office was on the floor directly above the location of British MI6.[7] In the earlier days of the war, Donovan cultivated a close relationship with Winston Churchill and Stewart Menzies, head of the British Secret Service, where he learned much of the art of spy craft from them.

In 1942, the COI became the Office of Strategic Services (OSS) and Donovan returned to active duty in the US Army with his WWI rank of Colonel. He was promoted to Brigadier General in March 1943 and to Major General in November 1944. The OSS consisted of men and women from many areas and backgrounds—lawyers, historians, bankers, baseball players, actors and businessmen. Under his leadership, the OSS would eventually conduct successful espionage and sabotage operations in Europe and parts of Asia by conducting in-depth research and analysis on the nation's enemies and their capabilities. However, the OSS continued to be kept out of South America as a result of Hoover's hostility to Donovan. In addition, the OSS was blocked from the Philippines by the antipathy of General Douglas MacArthur, the commander of the Southwest Pacific Theatre.[8]

Donovan was a fearless leader and became known for saying, "Let's give it a try!"[9] The OSS was instrumental in many of the successes during WWII, including providing the US government with advance information about German efforts to develop atomic weapons and the plot to assassinate Hitler.[10]

ROLE IN FORMATION OF THE CENTRAL INTELLIGENCE AGENCY

Towards the end of the war in 1945, Donovan tried to persuade both Presidents Roosevelt and Harry S. Truman to make the OSS a permanent civilian centralised intelligence agency, but his efforts were unsuccessful. The OSS was dissolved in September 1945. Donovan continued to advocate for the formation of a centralised intelligence agency. His persistence paid off when President Truman signed the National Security Act of 1947, which established the Central Intelligence Agency.

POST-WAR ERA

After the war ended, Donovan want back to his lifelong role as a lawyer to perform his last duty, to serve as Special Assistant to Chief Prosecutor, Robert H. Jackson at the Nuremberg War Crimes Tribunal. Donovan had the personal satisfaction of seeing Nazi leaders responsible for the torturing and capturing of OSS agents brought to justice. Donovan also strongly felt that German General Staff and Office Corps should not be prosecuted alongside the Nazi Leaders, but failed to get agreement from President Truman and so he resigned from the prosecution team.[11]

DEATH AND LEGACY

Donovan died from complications of vascular dementia on 8th February, 1959 at Walter Reed Army Medical Centre in Washington, at the age of 76 and was buried in Arlington National Cemetery. Major General Donovan was inducted into the Military Intelligence Hall of Fame in 1988.[12]

President Dwight D. Eisenhower referred to him as 'the last hero', which later became the title of a biography of him.[13] After his death, Donovan was awarded the Freedom Award of the International Rescue Committee.

The law firm which he founded in 1929, Donovan, Leisure, Newton & Irvine, continued well after his death and was only dissolved in 1998.[14] His home Chapel Hill near Berryville, Virginia, was listed on the National Register of Historic Places in 2004.[15]

CONCLUSION

William Donovan was a capable and respected leader who managed to live through two World Wars. The prestigious medals that he received during his lifetime are a testament to his vast contributions in the service of his country. Donovan was also very determined and intelligent, as seen from his efforts to create a centralised intelligence department from the start, to gathering information from around the world and using it to his country's advantage.

ENDNOTES

1. William J. Wild Bill Donovan, Major General, United States Army. Arlingtoncemetery.net; retrieved August 27, 2012.
2. Spinal Maingitis,.Corey Ford, *DONOVAN OF OSS* (Robert Hale, 1970).
3. Thomas A. Rumer, *The American Legion: A Official HIstory*, 1919–1989, New York: M. Evans and Co., 1990; pg. 107.
4. The Fighting 69th. http://www.sixtyninth.net/regiment.html.
5. Biography. A Look Back ... Gen. William J. Donovan Heads Office of Strategic Services. 2013. https://www.cia.gov/news-information/featured-story-archive/gen.-william-j.-donovan-heads-oss.html
6. *New York Times*. "James Montague, Versifier, Is Dead." 1941.
7. Anthony Cave Brown, *Wild Bill Donovan: The Last Hero*.1982.
8. Ibid.
9. Biography. A Look Back ... Gen. William J. Donovan Heads Office of Strategic Services. 2013. https://www.cia.gov/news-information/featured-story-archive/gen.-william-j.-donovan-heads-oss.html
10. Ibid.
11. Corey Ford, *DONOVAN OF OSS* (Robert Hale, 1970).
12. Biography. A Look Back ... Gen. William J. Donovan Heads Office of Strategic Services. 2013. https://www.cia.gov/news-information/featured-story-archive/gen.-william-j.-donovan-heads-oss.html
13. Evan Thomas, Spymaster General, http://www.vanityfair.com/culture/2011/03/wild-bill-donovan201103
14. Melody Petersen, Donovan, Leisure, Old-Line Law Firm , to Shut Its Doors, http://www.nytimes.com/1998/04/20/business/donovan-leisure-old-line-law-firm-to-shut-its-doors.html
15. National Register of Historic Places, https://npgallery.nps.gov/nrhp/Download?path=/natreg/docs/All_Data.html

Quotable Quotes

"History is a drama of the rise and fall of nations. Nations succeed when their people are united by a common will to survive, to face tough challenges together and to sacrifice self-interest for the greater good of society."
– Goh Chok Tong (b. 1941), former Prime Minister and Emeritus Senior Minister of Singapore

"The true soldier fights not because he hates what is in front of him, but because he loves what is behind him."
- G. K. Chesterton (1874-1936), English writer, poet, philosopher and biographer

"Appear weak when you are strong, and strong when you are weak."
- Sun Tzu (544-496 BC), Chinese general, military strategist and philosopher

"We are going to have peace even if we have to fight for it."
- Dwight D. Eisenhower (1890-1969), American politician and Army general
who served as 34th President of the United States

"A good plan violently executed now is better than a perfect plan executed next week."
- George S. Patton (1885-1945), Senior officer of the United States Army in World War II

"It is a mistake to look too far ahead. Only one link of the chain of destiny can be handled at a time."
- Winston Churchill (1874-1965), British politician and former Prime Minister of the United Kingdom

"Nearly all men can stand adversity, but if you want to test a man's character, give him power."
- Abraham Lincoln (1809-1865), American politician and lawyer who served as 16th
President of the United States

"The art of war is simple enough. Find out where your enemy is. Get at him as soon as you can. Strike him as hard as you can, and keep moving on."
- Ulysses S. Grant (1822-1885), 18th President of the United States

"Courage is the most important of all the virtues because without courage, you can't practice any other virtue consistently."
- Maya Angelou (1928-2014), American poet, memoirist, and civil rights activist

"You are braver than you believe, stronger than you seem, and smarter than you think."
- A. A. Milne (1882-1956), English author

"A leader is a dealer in hope."
- Napoleon Bonaparte (1769-1821), French military and political leader

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. 43 No. 2 [2017]

THE JOURNAL OF THE SINGAPORE ARMED FORCES