POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

Editorial Board

Advisor
RADM Giam Hock Koon

Chairman
COL Ng Wai Kit

Deputy Chairman
COL Irvin Lim

Members
COL (NS) Tan Swee Bock
COL Benedict Ang Kheng Leong
COL Lim Siong Tiong
ME7 Shue Pei Soon
LTC Huang Miaw Yi
ME6 Colin Teo
MAJ Charles Phua Chao Rong
MS Deanne Tan Ling Hui
MR Kuldip Singh
MR Daryl Lee Chin Siong
CWO Tang Peck Oon
MR Eddie Lim

Editorial Team

Editor
MS Helen Cheng

Assistant Editor
MR Bille Tan

Research Specialists
CPL Ong Marc-us
CPL Tan Wallace
LCP Kayson Wang
PTE Wu Wen Jie
PTE Zhu Lingkai
REC Joshua Foo

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© 2013 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.

Editorial

In this first issue of POINTER for 2015, we are pleased to present our 3 prize-winning essays from the 2013/2014 Chief of Defence Force Essay Competition (CDFEC). Our top prize winning essay, a collaboration effort by MAJ Phua Chao Rong, Charles and ME5 Seah Ser Thong, Calvin is entitled "Learning From Mother Nature: Biomimicry For The Next Generation Singapore Armed Forces (SAF)." This essay explores the possibilities of biomimicry and how it can be harnessed by the SAF. Biomimicry is defined as "....an approach to innovation that seeks sustainable solution to human challenges by emulating nature's time-tested patterns and strategies. The goal is to create products, processes, and policies—new ways of living—that are well adapted to life on earth over the long haul."[1]

While animals have supported human warfare for millennia, it may have appeared that the advent of metallurgy in modern militaries have displaced them with mechanical machines. However, according to the authors, the utility of animals has not diminished, especially in situations when the operating terrain does not favour metallurgy. The authors have cited various examples of the usage of animals in recent wars, for example, the US Army Special Forces had to improvise and call for precision-guided munitions while riding on horses to battle the Taliban forces in the mountainous terrain of Afghanistan. The authors have also given numerous examples in their essay where the potential of biomimicry can be harnessed. They conclude that notwithstanding the challenges of biomimicry, the 3rd Generation SAF can consider surveying biomimicry ideas and technologies and customising them to local needs.

MAJ Lee Hsiang Wei's "The Challenges of Cyber Deterrence" is the second prize winning essay. In his essay, MAJ Lee describes the three necessary pillars of cyber defence strategy—a credible defence, an ability to retaliate and a will to retaliate. According to MAJ Lee, the concept of cyber deterrence builds upon this strategy to alter an adversary's actions for fear of an impossible counter-action. He emphasises that cyber security is an expensive business and is a difficult strategy to achieve. Despite billions of dollars spent on cyber security, it has not stemmed the rise in cyber-attacks over the past five years. MAJ Lee argues that cyber deterrence is impractical for most nations, given today's technology and the lack of common interpretation of the international law for the cyber domain. His essay presents obstacles such as attribution, diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors and potential legal minefields which make cyber deterrence a difficult strategy to effectively operationalise.

The third prize winning essay is entitled "Armed Forces and Societies: Implications for the SAF" and is written by CPT Ren Jinfeng. In his essay, CPT Ren explains that the increasing professionalisation of the armed forces is a challenge to a nation's defence strategies and the armed forces is forced to adapt to socio-political changes, resulting in increasing inter-penetrability of civilian and military spheres and cultures. Because of this, CPT Ren feels that the military has to constantly review its structural relationship with society and strategic roles to anchor its legitimacy. Therefore, the SAF must continue to engage the larger civil society in defence policy issues, to encourage a greater sense of co-ownership and to sustain efforts in increasing the 'social capital' for the SAF. CPT Ren also examines the historical overview of the armed forces in societies, the decline of the conscription army during the post-Cold War period and the dominant trend in modern armed forces, as they adapt their roles, to strengthen the linkage to and the legitimacy in the society. He also studies the implications of such trends for the SAF.

Besides featuring the top three prize-winning essays from the 2013/2014 CDFEC, we are also pleased to present 4 essays which focus on cyberspace—cyber warfare, cyber attacks and cyber deterrence as a theme. Given reports of the growing number of major security breaches and hacker attacks globally as well as locally, we thought it would be timely to devote some attention to this very challenging issue.

"Hype or Reality: Putting The Threat of Cyber Attacks in Perspective" is by CPT Lim Ming Liang. In his

essay, CPT Lim highlights that the potential threat of cyber-attacks has been a subject of serious growing concern for many militaries and national security agencies. He cites the United States' experience, where the cyber threat is deemed a grave challenge that could seriously compromise the security of a nation to such an extent that it can be regarded as an 'act of war.' CPT Lim adds that there have been known cases of attacks against religious, corporate and government groups—formed by non-state cyber groups—and this has further heightened the urgent need for effective cyber security measures to be put in place. CPT Lim also highlighted various findings that question the plausibility for cyber-attacks to seriously compromise national security. CPT Lim's essay addresses the levels and measures of cyber threats, its limitations and the strategies against them, as well as instances of cyber-attacks targeted at states. His essay will also address the extent of the damage that can be caused by cyber threats.

The essay entitled, "Contested Territory: Social Media and the Battle for Hearts and Minds," is by CPT Lau Jian Sheng, Jason. In his essay, CPT Lau emphasises that throughout history, military forces around the world have faced a similar challenge—garnering civilian support for their activities. He explains that militaries are cognisant that their potency rests not only on their offensive capability, but also on the resolute backing of the entire population. Consequently, militaries are compelled to actively secure their wider public's commitment to defence. CPT Lau adds that this is a vital task even for the world's most powerful military, the United States. And, Singapore, as a much smaller state, is no exception. CPT Lau argues that the formulation of Total Defence as a security philosophy for Singapore was inspired by earlier models such as Switzerland's 'General Defence' and Austria's 'Comprehensive National Defence.' He notes that psychological defence is one of the five pillars of Total Defence and that the foundation for this robust pillar of psychological defence hinges on continual engagement with the populace and he assesses that the media's impact on fostering commitment to defence is therefore a critical success factor. In his opinion, Singapore's defence strategy that encompasses cultivating a national consensus may have come under mounting pressure in recent years, with media consumption patterns shifting from the mainstream mass media to online social media. CPT Lau concludes that in the long run, it is timely for the military organisation to open up to public dialogue in order to better communicate its purpose and mission to foster deeper personal engagement, to better prevail in the contest for hearts and minds; albeit a tight-fisted regulation of social media may yet win the battle but lose the war.

CPT Lim Guan He explores the issue of cyber defence further in his essay, "Cyberspace: What are the Prospects for the SAF?" According to CPT Lim, the development of cyberspace represents a rupture of security paradigms where state interests can no longer be so easily protected. He stresses that given the nature of cyberspace, the SAF faces challenges of interoperability at various levels. CPT Lim suggests the prospective elements which can form the basis of the SAF cyber strategy framework by studying three pillars of action—Resilience, Deterrence and Interoperability. He feels that a cyber strategy must also take into account three factors, i.e. environment, desired behaviours and actions. The purpose is to reconcile the offensive nature of cyber warfare with Singapore's defence interests, while leaving sufficient flexibility to assure freedom of operational manoeuvre in the cyber domain. To achieve this, CPT Lim emphasises that it is critical that the SAF rethinks its cyber architecture in order to maximise a spectrum of possible policy options for strategic interests, to help win the battle of tomorrow.

In the final essay, "How A Good Offence is not the Best Defence: An analysis of SAFs Approach to Cyber Warfare," LTA Ng Yeow Choon argues that technological advancement has ushered in an era of network-centric warfare where cyberspace plays an instrumental role in military operations. He elaborates that due to its integral nature to modern militaries, cyberspace offers the ideal platform on which military operators can conduct their missions. He further explains that cyber warfare refers to the military doctrines and tactics used by operators in their attempt to gain dominance in the realm of cyberspace. Through the analysis of the offensive and the defensive aspects of cyber warfare, LTA Ng argues that the SAF should invest in cyber-defence rather than cyber-offence. In addition, he also

suggests that by focusing on cyber-defence, the SAF may not only deter potential military aggressions from state actors but also protect Singapore's civilian infrastructure and institutions from non-state entities.

The POINTER Editorial Team

ENDNOTES

1. "What is Biomimicry?", Ask Nature, http://www.asknature.org/article/view/why_asknature

Learning from Mother Nature:
Biomimicry for the Next Generation SAF

by **MAJ Phua Chao Rong, Charles & ME5 Seah Ser Thong, Calvin**

Abstract:

This essay explores the possibilities of Biomimicry and how it can be harnessed by the Singapore Armed Forces (SAF). The usage of metallurgy in modern militaries appears to be devoid of a central essence and is often more a means to an end. Metallurgy works in binary terms; they either destroy or are destroyed, which does not reflect reality and nature's principles of growth and self-healing. However, the pursuit of biomimicry utilises innovative materials that injects life-like qualities into a weapon. This evolutionary bio-design is present in nature, not as a collection of parts but as a synthesis of a whole. As such, biomimicry may be a paradigm shift after metallurgy, in line with the humanity's quest of zealous discovery and technological advancement.

Keywords: Biomimicry, Technology, Harness, Combat Performance

INTRODUCTION

Animals have been man's best companion in warfare since ancient days. It was the cavalry horse, scout dog, messenger pigeon, amongst other animals that supported human warfare in the past millenniums.[1] However, the advent of metallurgy in warfare has displaced the now 'less reliable' animals with mechanical machines. Without metals, the materiel culture of society is unthinkable. Metallurgy is the basis for the production of the manufacturing, transportation and communications equipment, as well as for civil construction and military affairs.[2] What metallurgy gained in certainty, it lost in the human/animal touch and the unexplained irrational factors that animals deliver to the battlefield. As an old Chinese proverb goes – the warhorse was able to evade the enemy's pursuit independently and deliver its injured and even unconscious rider-owner back to base camp.

However, the utility of animals has not diminished, especially in situations when the operating terrain does not favour metallurgy. For example, during World War Two (WW II), American armoured units noted that the mountainous terrain and temperate forests in Sicily, Italy did not favour the mass use of armour.[3] Instead, the US forces adjusted and became mounted on horses. In the Asian theatre, the unorthodox combat unit, *'Merrill's Marauders'* used 340 horses and 360 mules to fight the Japanese in Burma.[4] The re-use of animals is not because of the immaturity of metallurgy. Most recently in the last Afghanistan war, the US Army Special Forces improvised and called for precision-guided munitions while riding on horses to battle against the Taliban forces in the mountainous terrain.[5]

Regardless of terrain, the lingering presence of animals is continually observed as an inspiration for military technologists throughout military history, and this trend is likely to continue. Biomimicry is the latest manifestation of this interdisciplinary introspection within academia-technologist community. Popularised around 1997 with the release of the book, *Biomimicry: Innovation inspired by Nature* by Janine M. Benyus, this burgeoning field will continue to serve future militaries. This essay seeks to explore the potential of biomimicry for the next generation SAF.[6]

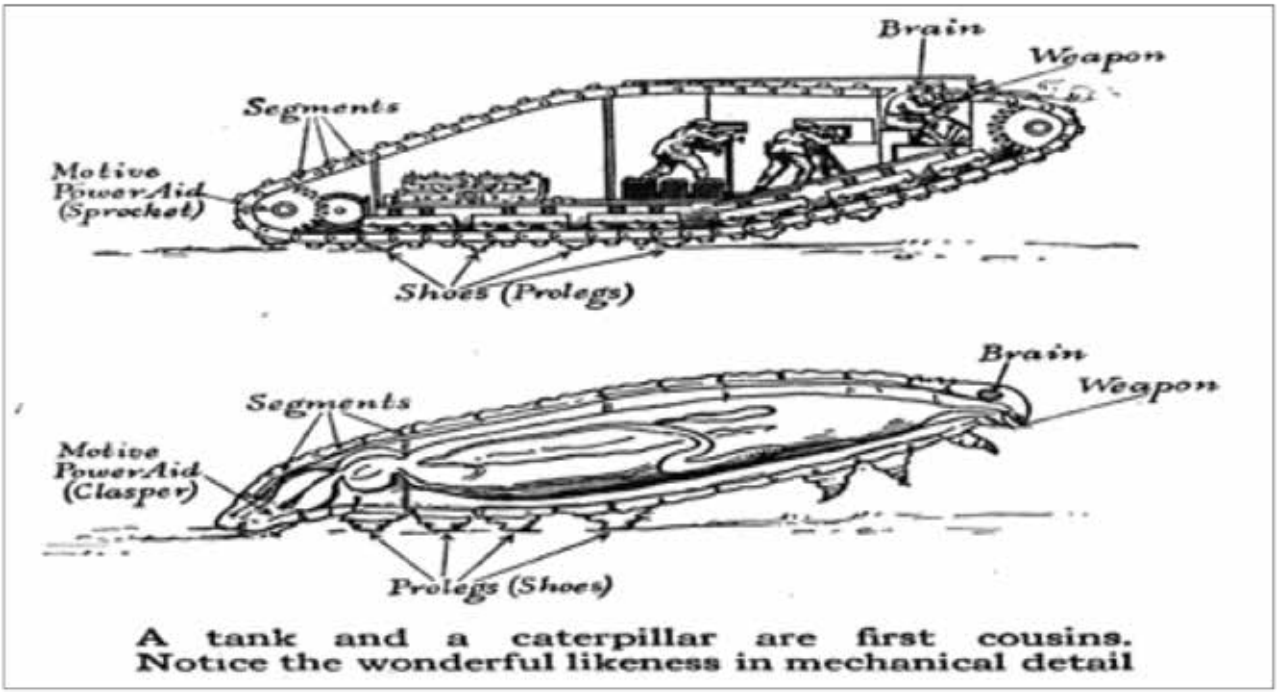


Figure 1: Prototype drawing of the 'Caterpillar tank'

DOMINANCE OF METALLURGY IN MODERN WARFARE

In modern militaries, most equipment are metallic. From precision strikes (small arms and large guns), to precision manoeuvres (soft and hard skin land vehicles, aircraft and ships) to precision information (ICK2 networks), all these equipment involve metals. Gone are the days where soldiers diligently practise martial arts to fight with spears in a phalanx formation or pikes (of which only the tip is metal) depending on the warrior culture and historical period. Metallurgy has now become the dominant paradigm in modern weapon technology.

Regardless of terrain, the lingering presence of animals is continually observed as an inspiration for military technologists throughout military history, and this trend is likely to continue.

That said, metallurgy appears to be devoid of a central essence and is often more of a means to an end. Animal mimicry, on the other hand, has often inspired and influenced the design of modern war machines. For instance, with reference to Figure 1, the first generation tanks took inspiration from caterpillars.[7] Modern radar (range and detection) mimicked the sonar mechanism used by bats and dolphins.[8] The Wright brothers would not have invented the prototype aircraft in 1903 if they had not attempted to mimic birds in flight; even Leonardo da Vinci's 'Ornithopter' and the Greek mythological character, Daedalus' fashioned wings of wax, feathers and twine, were a mimicry of birds.[9] As such, metallurgy is the means but animal mimicry was likely the source of inspiration to that end.

However, metallurgy may be ending with diminishing returns, typical in the 'S' curve of the technology life cycle and in its sustenance.[10] Given the advances of high technology, metallurgy may have lost its lustre. From a capability perspective, metals are hard with titanium as its best, but the hardest substance on earth is synthetic diamonds which costs about 15% less than real diamonds.[11] If not for the

cost, we would be shooting diamonds! Moreover, metal may be hard but it is less flexible and not stealthy, from the electronic detection means. Conceptually from a paradigm perspective, metallurgy appears to work in binary terms—metallic platforms either shoot or get shot, they either destroy or are destroyed. There is no fuzzy middle, such as growing and self-healing after being hit, which is hardly representative of reality and nature. The golden question is, what is next after metallurgy?

POTENTIAL OF BIOMIMICRY TO BE UNLEASHED

Imagine the following scenario unfolding in a night urban operation in which you are a lone soldier tasked to capture a terrorist in a building: While making your way to the building, your clothing changes patterns in accordance to your surroundings just like a chameleon. Upon reaching the building, you climb like a gecko to the 3rd floor where the terrorist is hiding. Once inside the building, you scan around and like a snake, you are able to sense the image of your target in the darkness. You move towards your target but he shoots at you. Your spider silk inner armour does not take a dent but your outer abalone shell outer armour self-heals; and you are able to move near enough to stun your target like an electric eel and capture him. While you carry your target out, you are able to avoid all the improvised explosive devices (IEDs) planted through your sense of smell. While the painted scenario is hypothetical, it may become a reality not too far into the future with militaries adopting biomimicry.

From an evolutionary perspective, biomimicry could be seen as the next military innovation/ RMA that has its weaponry rigorously tested by nature; animals' evolutionary change involves constant iteraton with nature and reality and as Charles Darwin's dictum goes, 'only the fittest survives'. From this chain of logic, by adopting biomimicry, SAF is able to indirectly harness nature's evolutionary force for our force development.

The paradigm of metallurgy dominance has yet to shift. But if it does, biomimicry is a possible successor. Nevertheless, even if it is only a complement to metallurgy at present, it is useful to understand the philosophical underpinnings and specific areas of contributions that biomimicry can offer for the next generation SAF.

From a philosophical perspective, biomimicry can be said to represent (philosophical) holism because bio-design, at present in nature, is not a collection of parts but a synthesis of a whole.[12] This is philosophically in sync with the 'system of systems' thinking of the Revolution of Military Affairs (RMA) since the 1990s with Network Centric Warfare.[13] Philosophically, animals are by nature a complete ecosystem (system of systems) and studying how animals 'operate' will help find parallels to which military technology and weaponry could emulate. From an evolutionary perspective, biomimicry could be seen as the next military innovation/RMA that has its weaponry rigorously tested by nature; animals' evolutionary change involves constant iteraton with nature and reality and as Charles Darwin's dictum goes, 'only the fittest survives'. From this chain of logic, by adopting biomimicry, SAF is able to indirectly harness nature's evolutionary force for our force development. This is in stark contrast to metallurgy where linearity and philosophical individualism appear to prevail. A digress to contrast physics and biophysics is needed in order to illustrate this case in point. Physics describes brute strength. In linear terms, it theorises that a well-fed 60kg top-notch weightlifter can carry about 180kg of weights, typically 3 times one's body weight, in a clean and jerk manner.[14] However, the wonders of biophysics reveals that a leaf-clutter ant can carry 50 times its own weight, a male rhinoceros beetle 850 times and a tiny mite 1,180 times its own weight.[15] The exoskeleton and biophysical make-up of these insects which operate in hordes has tremendous implications

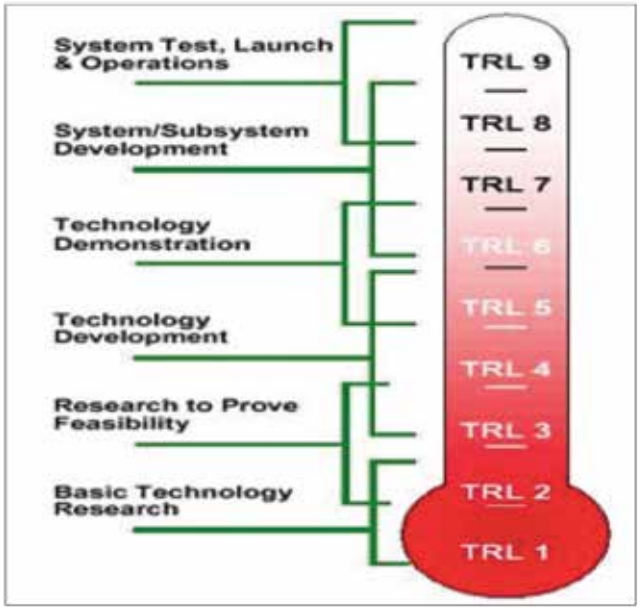


Figure 2: Technological Readiness Level

to military technology. Biophysics appears intriguing and full of potential.

A biomimicry design spiral, created by Carl Hastrich for the Biomimicry Institute is instructive to the holistic understanding of animals and derivation of implications for science and military technology.[16] The next section will discuss possible biomimicry ideas with respect to their Technological Readiness Level (TRL) for the next generation SAF. In Figure 2, the TRL is a measure used by selected United States (US) government agencies and many of the world's major companies and agencies to assess the maturity of evolving technologies, such as materials, components and devices, prior to incorporating that technology into a system or subsystem.[17]

BIOMIMICRY IN FUTURE ACTION (INDIVIDUAL SURVIVAL & PROTECTION)

Water Not Enough, No More.

Water is more critical than food. Humans die from dehydration within three to seven days, but can survive without food for more than 30-40 days. In battle, we must always foresee the scenario that an adversary will seek to cut off our lines of communications. Jungle survival skills teach us how to find water sources and drink from rivers using water purification tabs. However, what if there are no rivers and dynamic operations do not afford troops camping overnight to retrieve water from plants' condensation? Here, the Desert Beetles appear to have evolved a solution to this in the Namibian desert (see Figure 3). Though it lives in one of the driest deserts in the world, it is able to obtain all of the water it needs from the ocean fog due to the unique surface of its back. In the day, its matt black shell radiates heat; but at night, it becomes slightly cooler than its surroundings, causing fog to condense on its shell. In the morning, the beetle simply tips itself up, and lets the water trickle into its mouth. Designer Kitae Pak from the Seoul National University of Technology has designed the Dew Bank Bottle after the Desert Beetle and if further scaled down, it can enable war-fighters to harness water even in the most unlikely environments and empower our soldiers to fight and condense water on the move.[18]

Pixelated Camouflage Not Good Enough

In Soldiering 101, camouflage is used to prevent enemy detection. SAF has evolved from 1st to 2nd Generation camouflage, from using plants and synthetically pre-designed camouflage to digitally pixelated camouflage whose design has been proven by the US Marine Corps to play tricks with the human eye.[19] However, wearing the green pixelated uniform and fighting in an urban terrain do not intuitively translate to a sense of being 'protected' by the pixelated technology. Perhaps, the grey pixelated uniform would be useful in urban operations. However, it does not make logistical or operational sense to change from green to grey just before entering an urban terrain especially given the dynamic nature of next generation warfare whereby our soldiers are likely to have to fight in both urban and rural terrain interchangeably and in compressed tempo. Active or adaptive camouflage as inspired by chameleons and octopus is useful here. Chameleons [TRL: 4] and certain species of octopuses [TRL: 4] can alter their colour through the use of chromatophores that control the type and amount of light reflected. Work is being carried out by scientists at the Sandia National Laboratories in Albuquerque, New Mexico. The scientists have started to create a synthetic,

biomimetic material that will share the animals' ability to colour-shift. *"Military camouflage outfits that blend with a variety of environments without needing an outside power source - blue, say, when at sea, and then brown in a desert environment - is where this work could eventually lead to,"* says team leader George Bachand. [20]

BIO ARMOUR RULES FOR BOTH INDIVIDUAL AND PLATFORM PROTECTION

Currently, infantry soldiers wear heavy armour to protect against small arms fire, but this is at the expense of soldier mobility. Spiders offer a solution to light weight yet durable body armour. US scientists at the University of California have identified the genes and DNA sequences for two key proteins used in the 'dragline' silk of the tiny, but lethal, spiders found in the region. This discovery could lead to a variety of new materials for industrial, medical and military uses. Dragline silk from black widows [TRL: 4] is regarded as superior to that from other spiders because of its strength and extensibility, which enable the silk to absorb enormous amounts of energy. The silk's properties have interested the military, who are keen to explore the possibility of copying the structure of the silk for lightweight body armour.[21] This is not new per se given that what made the Mongols rule the steepe and the largest Empire in the world was their skill in horseback archery, manoeuvrist approaches and basic body armour of silk issued to every cavalry soldier.[22] As such, silk has already proven to be light enough yet resilient to protect themselves from enemy arrows. This Bio Armour is a new age rendition of that historical concept.

Figure 3. Desert Beetle and Dew Bank Bottle

Beyond lightness, the unique combination of fibre and exoskeleton in animals also prove to be useful if humans use exoskeleton to augment their human abilities. For instance, both the mantis shrimp [TRL: 4] and snail shell have [TRL: 3] inspired the composite use of hard ceramic and elastic organic materials. A partnership between Harvard University, the University of California and the Nanyang Technological University in Singapore has been established to study the makeup of the Mantis Shrimp's claw. They have found that the claw is made from a layer of very hard crystalline calcium-phosphate ceramic material that is about 60 µm thick. While it is actually quite fragile and would shatter on impact on its own, the team also discovered a much thicker region beneath it comprising layers of fibres made from an elastic material often found in sea fish exoskeletons. The team believed that the multiple layers of fibres have helped to prevent the claw from fracturing. With this design in mind, body armour could be designed in a similar way, using composites of hard ceramic and elastic organic materials.[23]

Besides Body Armour, Head Armour (helmet) is equally, if not more important since a head wound is an immediate evacuation from the battlefield. We often joke that 'one cannot think after putting on the helmet'. That is likely a comment in jest to illustrate the weight and discomfort from wearing a helmet, but the importance of a lightweight and durable helmet cannot be further underscored. Biophysical wonders in the woodpecker's skull design [TRL: 5], which enables it to withstand a shock of 60,000g of force without damaging the brain is useful here. Researchers at the University of California, Berkeley, have identified four designed safety features of woodpeckers. These four features combine to give strength and flexibility and yet minimise the transfer of vibrations as well as

reduce forces. These four features have been utilised in the design of new high impact products including crash helmets and flight data recorders.[24]

How about self-healing Armour? In metallurgy, the paradigm is binary opposites. Armour which has been destroyed has to be replaced entirely or risk being put out of action. But from a biological perspective, unless it is a serious third degree burn, the self-healing process of skin takes place. Such is the wonder of life—so why should our Armour be any different? The abalone shell [TRL: 4] is a case in point; besides being tasty, abalones shells are light yet extraordinarily tough—1,000 times more energy is required to break the shells than to fracture the toughest man-made ceramics. When cracked, the shells can even repair themselves. The abalone's toughness derives from layers of tiny calcium-carbonate plates that when struck, glide over one another to absorb the shock. If cracks develop, the plates simply grow back together. Princeton researchers are modelling the abalone's self-healing property in structures that can be built in space and similar principles could apply to military vehicles which are prone to damage in battle.[25]

BIOMIMICRY IN FUTURE ACTION (INDIVIDUAL COMBAT PERFORMANCE)

Scaling heights is No Longer a Feat

From an operational perspective, urban operations are difficult because buildings are hard to 'clear'. But a Gecko [TRL: 4] can scale up and down buildings effortlessly and its secret lies in the composite structure of its feet, on which every single toe pad is covered with millions of keratinous hair-like bristles called setae. Each seta in turn branches into hundreds of flat tips called spatulas, which make intimate contact with surfaces. This fibrillar array achieves adhesion primarily by non-covalent van der Waals forces between the spatulas and the surface. Theoretical van der Waals gloves could generate an adhesion force comparable to the body weight of 500 men.[26] If it was integrated into an Ant exoskeleton, it would grant tremendous strength, which one could scale buildings easily. Imagine how fast the SAF could clear buildings during Urban Operations.

'Who Says Dark Cannot Shoot!'

Currently, militaries fight with infra-red goggles but it frequently gets foggy in our tropical climate when we sweat, even at night! Bats [TRL: 6] use echo-location and snakes use pit organs to feel the presence of warm bodies. Based on the echo-location used by bats to find their way and avoid even small objects in total darkness, the UltraCane was developed to assist the vision impaired to find their way. It was designed and manufactured by Sound Foresight and uses sound waves to locate objects in front of the user. A small electronic echo-location device is attached to a white cane and provides sensory feedback through the cane's handle.[27] While this is currently used for the visually impaired, it could be adapted for soldiers who typically need to operate in the dark. If it is fashioned to work in combination with a soldier's weapon, the soldier could potentially find his way in the darkness and shoot instantly. In another study, scientists have discovered that vipers, pythons and boas [TRL: 3] have holes on their faces called pit organs, which contain a membrane that can detect infrared radiation from warm bodies up to one metre away. At night, these pit organs allow snakes to 'see' an image of their predator

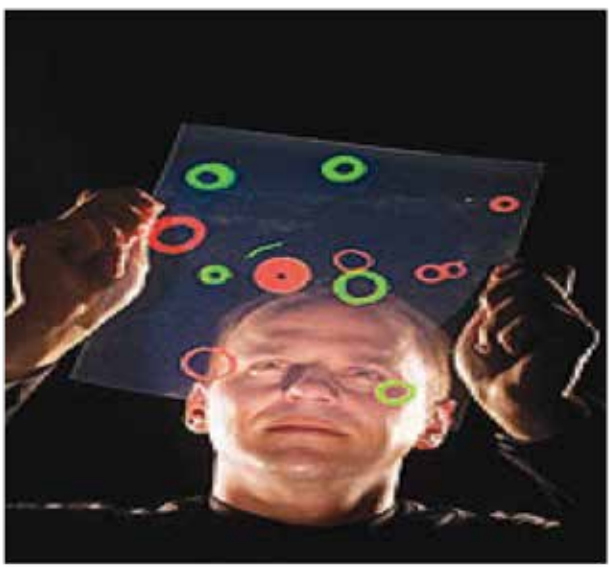


Figure 4. Sandia researcher George Bachand examines an enlargement of actual images of light-emitting quantum dots

or prey. This is akin to an infrared camera and may allow soldiers to see through camouflage that may fool the eyes.[28] This combination of localisation senses can complement our infra-red goggles to help SAF fight better in the dark and even through foliage (Foliage Penetration - FOPEN).

BIOMIMICRY IN FUTURE ACTION (SYSTEMS WARFARE)

Intelligence Warriors in the Animal Kingdom

Current militaries' intelligence assets composed largely of assets that extend the coverage of sight and sound beyond human limitations. With technological improvements, collection assets have reduced in size and improved in durability. However, this may pale in comparison to what the Animal Kingdom can deliver. Imagine, the Kingdom's Unmanned Aerial Vehicles (UAVs) are but flies [TRL: 8] which can take off and land in any direction, change course in just 30 thousandths of a second. It can use three different wing motions to create backspin and air vortices that create lift.[29] Land reconnaissance, bomb diffusion and counter-mining operations can be done by cockroaches [TRL: 5], who are apt in manoeuvring in different terrains undaunted by hip-height obstacles and slopes of up to 24 degrees.[30] They can be augmented by lobsters[31], [TRL: 4] for sea and land operations and silk-moths[32] [TRL: 3] for air operations, both of whose olfactory faculty are advanced enough to sniff out friends, foes and TNT. Lastly, imagine a horde of sand fleas [TRL: 4] jumping forward 30 feet into the air in cadence. The amount of comprehensive battlefield awareness would be unprecedented if the imagery captured by each sand flea is pieced together to form a macro-picture.[33] These are ideas that military nano technology can be developed further.

Or, what about the auto-sensing of chemical and biological threats? Here, the sensing capabilities of the Morphos butterfly [TRL:5] is a useful case in point. The Defence Advanced Research Projects Agency (DARPA) had awarded General Electric a $6.3 million grant to further develop a project to replicate the nano-structures from the wing scales of butterflies into sensors. Research has uncovered that the scales on Morphos butterfly wings can pick out molecules from the atmospheric noise. Such sensors could be embedded in clothing and tuned to change colour upon detection of a chemical or biological threats.[34]

Electronically Stealth Warfare for our Metallurgy

Modern warfare overly focuses on metallurgy and its natural nemesis is the radar. All metals will have a radar cross section (RCS) that 'bounces back' the radio waves to expose one's presence. Modern technology has tried to reduce this RCS through more graphite-based advanced materials, rounder edges and painting surfaces to absorb radiation, but RCS is still present.[35] All moths have anti-reflective (AR) surfaces and have inspired the creation of anti-reflective, radio frequency transparent windows. The surface of a moth's cornea consists of tiny protruding bumps that exist to keep moths safe from predators, by preventing light from reflecting in their eyes and betraying their presence. Mark Mirotznik, from the University of Delaware, has adapted these AR ideas and created special surfaces in which microwave energy is transmitted with very little reflections over large ranges of frequency or bandwidths. Special windows can then be created which can enable an antenna system within to transmit, yet at the same time prevent radar detection. [TRL: 4][36]

Unmanned Warfare – the 'Animal' Way

Unmanned warfare is the latest fad in warfare. UAV drones allegedly spied on Osama bin Laden the night before the special operations raid that killed him in Pakistan.[37] Our Combat Engineers use robots as unmanned land vehicles to assist in Chemical, Biological, Radiological and Explosive (CBRE) operations. Now, imagine unmanned land vehicles as fast as the cheetah and armed with weaponry. The cheetah is the fastest land animal with a sleek body that is built for speed. It is also the name for a four-legged robot under development by Boston Dynamics, which can run faster than humans. DARPA awarded the company a contract to build a faster, more fearsome animal-like robot. Boston Dynamics has envisioned Cheetah performing military operations

Figure 5. Boston Dynamics' Cheetah Robot

with excellence, with its incredible agility to make tight turns so that it can zigzag to chase and evade and have the ability to stop suddenly. [TRL: 8][38]

Cyber Defence – the 'Ant' Way

Information Knowledge-Enabled Command and Control (IKC2) and Network-Centric Warfare are about networked-enabled warfare where precise information manoeuvres and fires are made possible by Information Communication Technology (ICT). The flip side of it is that adversaries only need to cripple one's IT systems to disable its military. Hence, Cyber Defence is important and the SAF has also recently announced its focus in this area.[39] The operating concept of Ants can inspire us on this security journey. By looking at the way ants call for backup and overpower invaders through sheer quantity of soldiers, security experts have devised the 'digital ant' [TRL: 6], that will help human operators spot threats to computer systems more quickly. Unlike traditional security devices, which are static, these 'digital ants' wander through computer networks looking for threats, such as 'computer worms'—self-replicating programmes designed to steal information or facilitate unauthorised use of machines. When a 'digital ant' detects a threat, an army of ants will converge at the location and help draw the attention of human operators who can step in to investigate. Whenever a 'digital ant' identifies some evidence, it is programmed to leave behind a stronger scent to attract more ants and thus produce the swarm that marks a potential computer infection. So far, experiments with the 'digital ants' have been successful. The technology fits best for large computer networks for corporations, universities and militaries. Soon, we may just owe the security of our computers to the often underestimated 'digital ant.'[40]

Biomimicry presents exciting possibilities for military technology and is an unconventional form of technology that the next generation SAF should keep a watch on.

WHITHER PARADIGM SHIFT FOR NEXT GENERATION MILITARIES?

Biomimicry presents exciting possibilities for military technology and is an unconventional form of technology that the next generation SAF should keep a watch on. However, biomimicry is not without its challenges. Akin to most Research and Development (R&D) efforts, extensive resources such as time and money are essential. And yet, results may be uncertain even with an abundance of these as there are many uncertainties in learning from nature, which is a whole system by itself.

Notwithstanding its challenges, the 3rd Generation SAF can consider experimenting with some of the seed ideas in our local context. To enable this, military technologists can take up roles akin to DARPA to bridge research between academia, commercial companies and the military. Collaborations through these networks will better allow the SAF to survey biomimicry ideas and technologies and customise them to local needs. To this end, Future Systems and Technology Directorate (FSTD) is well-poised for this role.

Whether biomimicry will prove to be the next paradigm shift after metallurgy will depend on the FSTDs around the world and their diligence in breaking through the mindset that warfare involving metallurgy and fires is the most reliable mode. This assumption may no longer be relevant. When China invented fire powder and used it for celebratory fireworks in the Song dynasty, the Europeans were happily fighting with pikes and swords in the Middle Ages.[41] It was the

curiosity and willingness to venture into uncharted waters that enabled these scientific breakthroughs. The same can be same for the invention of the atomic bomb during WW II. One thing is clear: nature is unique and wonderful. Learning from and about nature, since the Age of Enlightenment, has led to immense knowledge creation of the modern day. The attempt to adopt biomimicry for the next generation SAF is in line with this never-ending human quest of introspective learning and zealous discovery.

ENDNOTES

1. C. Michele Hollow and William P. Rives, VMD, "Animals in the Military," *Netplaces*. http://www.netplaces.com/working-with-animals/to-the-rescue/animals-in-the-military.htm.
2. *The Great Soviet Encyclopedia*, 3rd Edition, The Gale Group, 1970-1979.
3. Steven J. Zaloga, *US Armoured Units in North Africa & Italian Campaign* 1942-45 (Oxford: Osprey Publishing, 2006), 84.
4. Roman Jarymowycz, 'Cavalry in the Second World War: The Horse within Blitzkrieg', in Roman Jarymowycz, *Calvary: From Hoof to Track*, (PA: Stackpole Books, 2008), 184-192.
5. John A. Nagl, *Counterinsurgency Lessons from Malaya and Vietnam: Learning to Eat Soup with Knife,* (Westport: Praeger, 2002), xiii.
6. Janine M. Benyus, Biomimicry: *Innovation inspired by nature,* (New York: William Morrow & Company, 1997).
7. John Walker Harrington, "Why tanks are giant caterpillars," *Popular Science Monthly* 92, (Jan-Jun 1918). http://www.popsci.com/science/gallery/2011-01/archive-gallery-best-biomimicry?image=2.
8 Knowledge@Wharton, "Learning from Sharks and Spiders: The Hand of Nature in Innovation," 1 Mar 2000. http://knowledge.wharton.upenn.edu/article.cfm?articleid=144.
9. Wendy Priesnitz, "Education Inspired by Nature," *Life Learning Magazine,* January/February 2011.http://www.lifelearningmagazine.com/1102/education_inspired_by_nature.htm.
10. A. Sood, *Technology S-Curve,* Wiley International Encyclopedia of Marketing, 2010.
11. Elsa Wenzel, "Synthetic diamonds still a rough cut," *CNET,* 14 Feb 2007 http://news.cnet.com/Synthetic-diamonds-still-a-rough-cut/2100-11395_3-6159542.html.
12. Michael Mehaffy and Nikos A. Salingaros, "The Radical Technology of Christopher Alexander," *Metropolis,* 6 Sep 2011. http://www.metropolismag.com/Point-of-View/September-2011/The-Radical-Technology-of-Christopher-Alexander/index.php?tagID=516.
13. Report of a conference organized by the *Institute of Defence and Strategic Studies* (IDSS) on 'Revolution in Military Affairs: processes, problems and prospects," 22-23 Feb 2005.
14. David Segal, "Where the Heavy Lifting Often Occurs in the Mind," *The New York Times,* 1 Aug 2012. http://www.nytimes.com/2012/08/02/sports/olympics/for-olympic-weight-lifters-event-is-more-than-momentary-lift.html?pagewanted=all&_r=0.
15. Jeremy Coles, Humans vs Ants: Animal Athletes in Action, 3 Aug 2012. http://www.bbc.co.uk/nature/18996429.
16. Biomimicry Institute, "Design Spirals," *Biomimicry Guild,* 2008. http://www.biomimicryinstitute.org/downloads/DesignSpirals.pdf.
17. Airspace Systems, "Technology Readiness Levels Introduction," 21 October 2004. http://web.archive.org/web/20051206035043/http://as.nasa.gov/aboutus/trl-introduction.html.
18. New Idea Homepage, "Weird Beetle In the Desert That Collects Water, 10 Jul 10. http://www.inewidea.com/2010/07/10/32102.html.
19. Olive-Drab, "Marine Pattern Uniform (MARPAT)," 12 Oct 2011. http://olive-drab.com/od_soldiers_clothing_marpat.php.
20. "21st-Century Camouflage," Army-technology.com, 11 Feb 2011. http://www.army-technology.com/features/feature109521/.
21. Agençe France-Presse , "High-tech armour from widow spider silk?," *COSMOS Magazine,* 15 Jun 07. http://www.cosmosmagazine.com/news/1389/high-tech-armour-widow-spider-silk.
22. Timothy May, *The Mongol Art of War,* Pen & Sword Military (2007).

23. Timon Singh, ""Super-Strong Mantis Shrimp Could Inspire New, Tougher Body Armor," *Inhabitat,* 11 Jun 2012. http://inhabitat.com/super-strong-mantis-shrimp-claw-could-lead-to-stronger-body-armour/.

24. Paul Marks, "Woodpecker's head inspires shock absorbers," *New Scientist,* 09(2798): 21, 2011. http://www.discoveryofdesign.com/id52.html.

25. John Greenwald, "Learning at Mother Nature's Knee," *Fortune Magazine,* 22 Aug 2005 Issue.

26. Pugno, Nicola M, "Spiderman Gloves." *Science Direct: Nano Today* 3, 5-6. (2008). http://www.sciencedirect.com.

27. Buzzle Staff and Agencies, "Biomimicry - The Science of Copying Natural Designs," Buzzle.com. http://www.buzzle.com/articles/biomimicry-the-science-of-copying-natural-designs.html.

28. Janet Fang, "Snake infrared detection unravelled," Nature, 14 Mar 10. http://www.nature.com/news/2010/100314/full/news.2010.122.html?s=news_rss.

29. Squatriglia Chuck, "Spy Fly: Tiny, winged robot to mimic nature's fighter jets," *SF Gate,* Tuesday, 2 Nov 1999.

30. JE Clark, Cham JG, Bailey SA, Froehlich EM, Nahata PK, Full RJ, Cutkosky MR, 'Biomimetic Design and Fabrication of a Hexapedal Running Robot', *IEEE International Conference on Robotics and Automation,* 2001.

31. Louise Knapp, "Robo Lobster to Sniff Out Mines," Wired.Com, 2 Jan 02. http://www.wired.com/science/discoveries/news/2002/01/48892?currentPage=all.

32. Tina Casey, "Silkmoth Inspires New Attack on Bomb Detection," *Clean Technica,* 3 Jun 12. http://cleantechnica.com/2012/06/03/silkmoth-inspires-biomimicry-explosives-detector/ .

33. Timon Singh, "Boston Dynamics' Sand Flea Robot Can Jump 30 Feet Into the Air," *Inhabitat,* 4 Feb 12. http://inhabitat.com/boston-dynamics-sand-flea-robot-can-jump-30-feet-into-the-air/.

34. *Mobile Magazine,* "Darpa's Butterfly: Inspired sensors light up at chemical threats," 13 Aug 10. http://www.mobilemag.com/2010/08/13/darpa%e2%80%99s-butterfly-inspired-sensors-light-up-at-chemical-threats/.

35. Aerospaceweb.org, "Radar Cross Section." http://www.aerospaceweb.org/question/electronics/q0168.shtml.

36. Karen B. Roberts, "Moth eyes inspire antireflective surfaces for military applications," *Phys Org,* 8 Mar 2011. http://phys.org/news/2011-03-moth-eyes-antireflective-surfaces-military.html.

37. Aamer Madhani and Yochi J. Dreazen, , "Step by Step: How the U.S. Killed bin Laden," *National Journal,* 3 May 11. http://www.nationaljournal.com/nationalsecurity/step-by-step-how-the-u-s-killed-bin-laden-20110503.

38. Peter Farquhar,"Robot Cheetah used to dodge. Now it hunts," news.com.au, 6 Mar 12. http://www.news.com.au/technology/sci-tech/robot-cheetah-used-to-dodge-now-it-hunts/story-fn5fsgyc-1226290441182.

39. MINDEF, Keynote Address by Dr Ng Eng Hen, Minister for Defence, at the DSTA-DSO Scholarship Award Ceremony, Official Release, 2013, 24 Jul 13. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2013/24jul13_speech.html.

40. Jaymi Heimbuch, "New Biomimicry in Digital Security - Ants Swarm to Protect Computers," *TreeHugger,* 28 Sep 09. http://www.treehugger.com/clean-technology/new-biomimicry-in-digital-security-ants-swarm-to-protect-computers.html.

41. EconomicExpert.Com, "Fire Work." http://www.economicexpert.com/a/Fireworks.htm.

ME5 Calvin Seah is currently attending the 46th Command & Staff Course. He is an Army Engineer by vocation. ME5 Seah holds a Bachelors of Engineering in Mechanical & Production Engineering from NTU, Masters of Science in Industrial and Systems Engineering from NUS as well as a Masters of Science in Defence Technology and Systems from NUS, obtained under the SAF Postgraduate Award.

He is a Business Excellence Assessor, National Innovation and Quality Circle Assessor as well as an American Society of Quality Judge. He was a winner of the 1st and Merit Prizes for his co-written essays at the CDF Essay Competition 2013/2014 and a winner of the Commendation award at the 15th COA Essay Competition in 2014.

MAJ Phua Chao Rong, Charles is currently doing his PhD at the Lee Kuan Yew School of Public Policy (LKYSPP) on a NUS Lee Kong Chian Graduate Scholarship. An Academic Training Award (Overseas) recipient, MAJ Phua holds a Masters of Science (Research) with Merit and a Bachelors of Science (2nd Upper Honours) in International Relations from the London School of Economics and Political Science (LSE). He is a recipient of the Global Sachs Global Leaders Award (2004) for academic and leadership excellence at LSE and has also received the HSBC Youth Excellence Award (2005) for youth leadership and community service from President S R Nathan. A seven-time Commendation Award winner in the CDF Essay Competition and a three-time Outstanding Award winner in the Chief of Army Essay Competition, he has also published in the Royal United Services Institute (RUSI) Journal, Military Review, POINTER and co-authored a chapter in an Institute of Policy Studies (IPS) publication. He is currently the Editor-in-Chief of Asian Journal of Public Affairs (LKYSPP's flagship journal) and Assistant Editor of Comparative Public Policy Series (Cambridge University Press). He is Founder/President of LKYSPP-Association for Public Administration.

The Challenges of Cyber Deterrence

by **MAJ Lee Hsiang Wei**

Abstract:

In the cyber realm, there are three necessary pillars of cyber defence strategy—a credible defence, an ability to retaliate and a will to retaliate. The concept of cyber deterrence builds upon this strategy to alter an adversary's actions for fear of an impossible counter-action. Cyber security is an expensive business and is a difficult strategy to achieve. Despite billions of dollars spent on cyber security, it did not stem the rise in cyber-attacks over the past five years. Cyber deterrence is impractical for most nations given today's technology and the lack of common interpretation of the international law for the cyber domain. This essay presents obstacles such as attribution, diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors and a potential legal issue that make cyber deterrence a less viable strategy to adopt.

Keywords: Cyber Security, Cyber Deterrence, Viability, Technology, Hacker

INTRODUCTION

The threat of cyber-attacks and the ascent of cyberspace as a military domain has gained significant traction over the past three years. The Stuxnet computer worm was discovered in June 2010 and it was found to specifically target Iran's nuclear enrichment centrifuges.[1] The extent and complexity of Stuxnet demonstrated the potential of cyber warfare and the extent it could be used. The use of cyber warfare was also evident in conflicts both in Estonia and Georgia, in 2007 and 2008 respectively, where coordinated cyber-attacks compromised government websites and denial of service attacks crippled the systems of news networks and financial institutions.[2] More recently, the threat of cyber-attacks and subsequent defacement of Singapore government websites by 'The Messiah' in October 2013 showed that Singapore was not spared in the realm of cyber-attacks.[3] The cost of cyber defence has also garnered significant attention with reports of countries spending billions of dollars on cyber defence in a single year.[4] With the increased awareness of cyber-attacks and cyberspace as a military domain, the concept of cyber deterrence has gained traction amongst countries such as the United Kingdom and the United States.[5]

The concept of cyber deterrence builds upon the strategy of cyber defence by incorporating both the ability to retaliate as well as the will to retaliate towards the cyber attacker. This essay will argue that the concept of cyber deterrence is impractical for most nations given today's technology and the lack of a common interpretation of the international law for the cyber domain. While academics have well-articulated the elements of deterrence, in practice there are implementation hurdles and practical problems that would render most proposed cyber deterrence strategies inimical to a nation's interests. A credible cyber defence, though probably more expensive, is a less risky and more practical approach.

What is a Cyber-attack?

One can view a cyber-attack as any action taken to undermine the functions of a computer network for a political or national security purpose.[6] For a cyber-attack to be carried out, it usually requires the target

system to have one or more vulnerabilities that the attacker can exploit to manipulate to the system. Some of the vulnerabilities used are known as 'zero-day' as they had not been uncovered or made known to the developers. Stuxnet, for example, was found to use a total of four zero-day vulnerabilities.[7]

What is Cyber Deterrence?

According to conventional deterrence theory, "deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[8] The strategy of deterrence gained prominence in the Cold War model of Mutually Assured Destruction where any nuclear attack would be met with an overwhelming nuclear counter strike that would also destroy the aggressor. Hence, deterrence really is about the ability to alter an adversary's actions by changing the attackers' cost-benefit calculations that includes subjective and psychological assessments, as well as a state of mind brought about by the existence of a credible threat of unacceptable counteraction.[9]

With the increased awareness of cyber-attacks and cyberspace as a military domain, the concept of cyber deterrence has gained traction amongst countries such as the United Kingdom and the United States.

Extending this concept of deterrence to the cyber realm, cyber deterrence seeks to dissuade the attacker from acting for fear of retaliation. It requires preparedness and a degree of retaliatory certainty, which is linked to having an offensive capability.[10] In the cyber realm, there are three necessary pillars in this strategy—*a credible defence, the ability to retaliate and the will to retaliate*.[11] See Figure 1.

The first pillar of an effective cyber deterrence strategy is to have a *credible defence*. If the cyber defence of a country is sufficient to make an attack exceedingly difficult, an attacker might decide that he lacks sufficient expertise or choose to give up after multiple failed attempts.[12] In addition to preventing a successful cyber-attack, a credible defence is also about having backup systems to achieve 'defence in depth' such that a single successful attack would not result in a total loss of the system.[13] This goal, although expensive,[14] is a practical solution to the majority of attacks.[15]

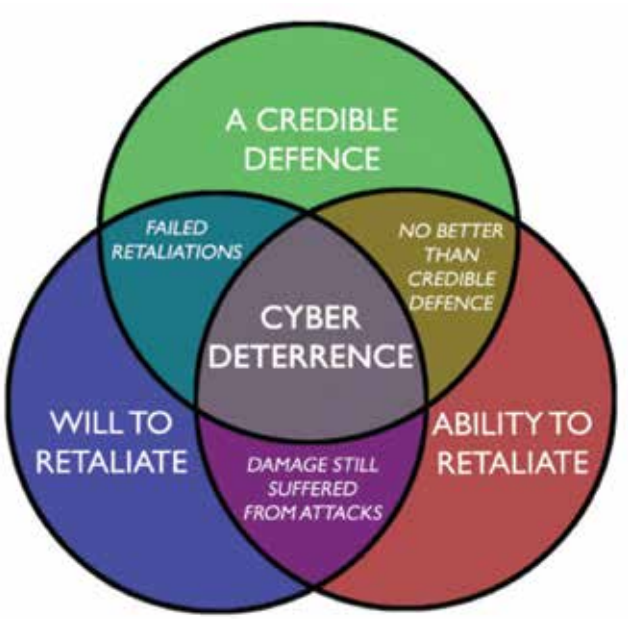


Figure 1: Components of Cyber Deterrence

The next pillar is *the ability to retaliate*. For this pillar to work, the retaliatory action would need to result in damage greater than that inflicted by the attacker.[16] In the cyber domain, this refers to the ability to carry out cyber-attacks unto the original attacker. Implicit to the ability to retaliate in the cyber domain is the ability to identify the cyber attacker.

The last pillar is *the will to retaliate* against potential cyber attackers. The will to retaliate needs to be an overt policy. For cyber deterrence to work, the cyber attackers need to be dissuaded when they include the possibility of cyber retaliation into their impact calculus. If the perceived possibility of retaliation and the pain from cyber retaliation is high, the cyber attacker may be dissuaded from attacking. As such, the nuancing of the will to retaliate is crucial

to the success of a cyber-deterrence strategy. If the message is too indeterminate, hawkish or directed to the wrong party, the will to retaliate may be rendered ineffective.[17]

A Case for Cyber Deterrence?

Given that cyber security is an expensive business and the goal of cyber deterrence would be to reduce the risk of cyber-attacks to an acceptable level at an acceptable cost, cyber defence is expensive.[18] An estimated US$55 billion was spent on cyber security in 2011 and the amount is expected to rise to US$86 billion in 2016.[19] Another study also attempted to place the cost of cyber security into perspective, estimating that an average of US$10 million was invested in cyber defence for every 125 lines of attack code written.[20] Unfortunately, expensive investment did not stem the rise in cyber-attack incidents over the past five years (See Figure 2).[21]

Governments around the world are continuing to commit more dollars in the area of cyber security. Under President Obama, the US had increased the budget for cyber defence by US$800 million to US$4.7 billion in 2014, despite tightening US budget

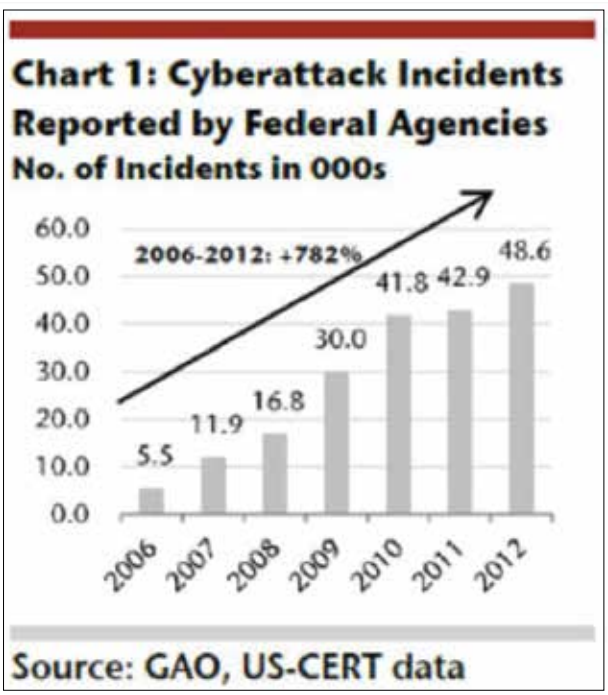


Figure 2: Cyber Attacks Incidents on US Federal Agencies

constraints.[22] The Director of the Federal Bureau of Investigation (FBI), James B. Comey, even cautioned in a meeting with the Senate Homeland Security and Governmental Affairs Committee that in the future, "resources devoted to cyber based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats."[23] The Singapore government had done likewise in 2013 with a S$130 million plan to enhance the nation's cyber security.[24]

In addition, there are reports claiming that several countries such as India, China, North Korea as well as Pakistan, are rapidly developing their cyber offensive capability.[25] Some countries,[26] such as Iran,[27] have openly declared similar intentions. The threat of cyber-attacks will continue to increase as more countries develop cyber offensive capabilities.

OBSTACLES IN ACHIEVING CYBER DETERRENCE

On a conceptual level, the pillars needed to support the strategy of cyber deterrence may seem intuitive. However, the implementation and execution of the cyber deterrence strategy is inherently problematic. These obstacles affect *the will to retaliate* and *the ability to retaliate* in the cyber domain.

Problem of Attribution

The notion that retaliation can only take place after the attacker is identified tends to be trivialised as identification of the attacker is assumed to be fairly straightforward in traditional warfare. In the cyber domain however, tracing the source of cyber-attacks can be a significant hurdle. General Keith Alexander, Commander of the United States Cyber Command, mentioned in a testimony to the US Congress in 2010 that even in the foreseeable future, attribution of cyber-attacks will likely remain "costly and comparatively rare."[28]

The Stuxnet computer worm that targeted Iran's nuclear centrifuges in 2010, exemplifies the difficulty in determining who the actual attackers were. Although the US and Israel were widely believed to be behind Stuxnet, there had not been any concrete evidence

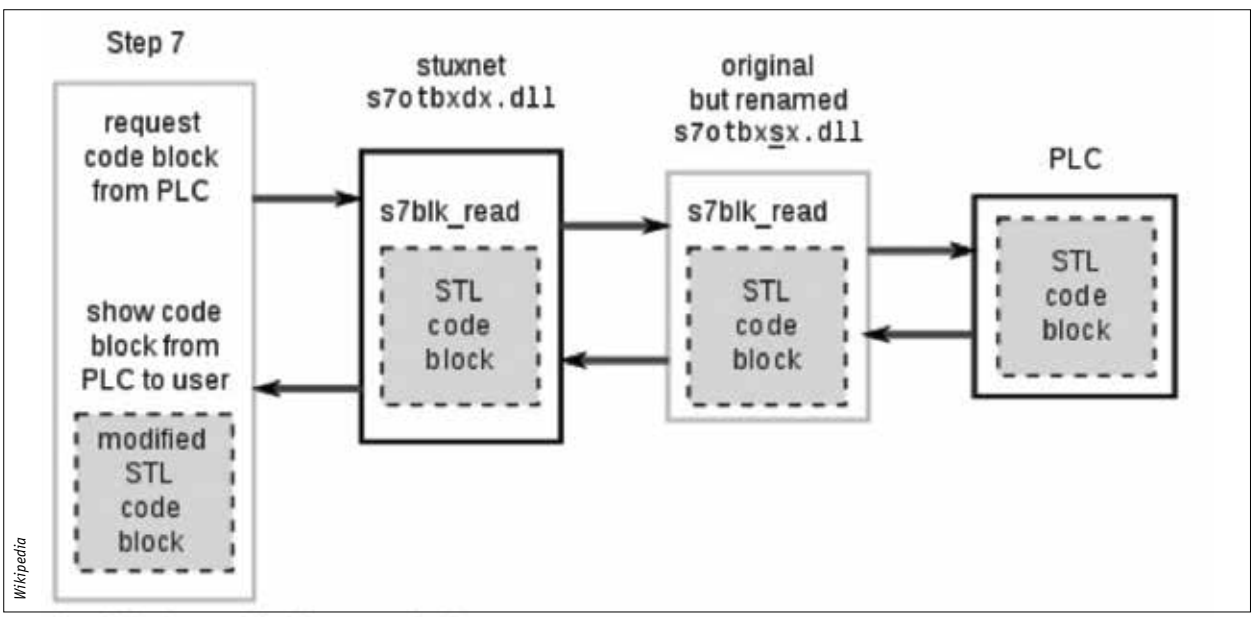
supporting this assertion.[29] Most of the allegations stemmed from weak circumstantial hypotheses. An example of such weak links is concerning the use of the term 'myrtus' in the Stuxnet code.[30] The term 'myrtus' can either be linked to a story of a Persian plot against the Jews in the Bible's Book of Ester or simply an abbreviation for 'my Remote Terminal Units' (my-RTUs). Even after months of in-depth analysis by established security firms such as Symantec, Kaspersky Labs and F-Secure, the attacker behind the Stuxnet malware could not be definitively identified. Even while Edward Snowden had indeed claimed in an interview that Stuxnet was a collaborative effort between the United States and Israel, there has not been any further evidence available to back up the claim.[31]

The main reason why identifying a cyber-attacker is often times challenging is because almost anyone could be the culprit.

The main reason why identifying a cyber-attacker is often times challenging is because almost anyone could be the culprit. The equipment needed to launch a cyber-attack is easily accessible and inexpensive. Also, cyber-attacks can be launched from almost anywhere—an open Wi-Fi access point, a compromised third party computer or even a stolen mobile phone and routed through multiple servers before reaching the intended target. As such, attribution is often guesswork. Even with the improving ability to trace the source of cyber-attacks in recent years, computer security experts acknowledge that it is still difficult to identify the cyber attacker with total certainty.[32]

For deterrence to work, potential attackers must be sufficiently concerned that their identity would be exposed and retaliation carried out on them. Misattribution and incorrect retaliation not only weakens the logic of deterrence, but possibly results in a new enemy. The prospect of facing one cyberwar against the original attacker would have evolved to two cyberwars against both the original attacker and the misattributed party.[33]

The ability to correctly attribute the source of a cyber-attack is a key element of the cyber deterrence strategy. If a nation has doubts over the accuracy of the attribution, it would negate the will to retaliate. Retaliating against an innocent party would run the risk of unwanted escalation. If a nation is unable to confidently identify the attacker, there is no way



Overview of the Stuxnet hijacking communications

a retaliatory attack can be launched and hence the ability to retaliate will be effectively nullified.

The technology to accurately attribute cyber-attacks may exist outside of the open-source realm and is by extension, a closely guarded secret. The existence of such undisclosed ability to accurately attribute the cyber-attack does not play a role in deterring potential cyber attackers. Firstly, the cyber attacker, without knowing the defender's ability to attribute accurately, would not be otherwise deterred from attacking. Secondly, if the attacker believes the retaliator is just guessing or that the retaliator has ulterior motives for retaliating, the conclusion may be that carrying out further attacks will have no effect on whether or not it will face further punishment.[34] The strategy of cyber deterrence would have failed in both scenarios.

Diminishing Capability to Retaliate

Unlike a nuclear retaliatory attack, it is difficult to imagine an act of cyber retaliation that is so overwhelming that no potential cyber attacker would run the risk of being hit. Hence, repeated cyber retaliation may sometimes be necessary to enforce cyber deterrence. Computer vulnerabilities are often patched and removed expeditiously after their discovery.[35] It is unlikely for a vulnerability to go unpatched for extended periods especially after a malware has inflicted damage on well-defended systems. Even if the cyber attacker is able to produce variants of the malware, the defender would be attuned to detection and the variants would have far less effect. Academics at RAND Corporation have even gone as far as to call cyber-attacks a 'one use weapon.'[36] This characteristic is detrimental to achieving cyber deterrence as a successful retaliation may not be convincing if the attacker, who would perform the necessary security updates, believes it will be less vulnerable the next time around.

While it may be argued that since cyber retaliation is in itself a form of cyber-attack and the diminishing returns on successive offensive actions affect both

Unlike a nuclear retaliatory attack, it is difficult to imagine an act of cyber retaliation that is so overwhelming that no potential cyber attacker would run the risk of being hit. Hence, repeated cyber retaliation may sometimes be necessary to enforce cyber deterrence.

parties—the original attacker and the defender, it is important to recognise that the luxury of time to uncover and accumulate multiple vulnerabilities in the target system lies with the attacker rather than the defender carrying out cyber retaliation.

Conceptually, for a nation to maintain the ability to retaliate timely, it first has to be able to identify the list of potential cyber attackers and then collate and continuously update an associated library of vulnerabilities. The library of vulnerabilities may be large due to the number of countries with cyber offensive capabilities themselves. Publicly available information shows 46 countries with military cyber programmes, with 11 counttries having offensive cyber capabilities in 2012, up from four in 2011. Many more countries could well have military programmes but do not admit to them.[37] Since vulnerabilities are constantly being discovered and corrected, the useful life of an exploit may be limited. As such, maintaining a potentially large library of vulnerabilities could place undue strain on intelligence requirements.[38]

Avoiding Escalation

The aftermath of a successful retaliation against an initial cyber-attack is difficult to predict or control. A mistimed or misinterpreted action could well result in the escalation of the situation, resulting in more cyber-attacks. The timing, choice, scope and nature of the retaliation would affect the perceived message by the attacker.

Adding to this complexity in messaging, the difficultly in tracing the source of the cyber attacker

can take up to several months. This will result in a delay between the attack and the retaliatory action. The act of cyber retaliation may itself take months to execute before the effects are felt and noticed by the attacker. By the time the retaliatory cyber-attack is discovered, the retaliation could possibly seem both arbitrary and unrelated to the original incident.

If the messaging had indeed been misinterpreted, the defending nation would run the risk of the attacker responding by escalating the matter to an armed conflict. If the attacker becomes convinced that he would lose the cyber tit-for-tat, the option to counter retaliate in a different domain becomes an inviting proposition.[39] In 1998, it was reported that Russia, being concerned about their ability to control 'information warfare,' was openly declaring that it reserved the option to react to a strategic cyber-attack with the choice of any weapon in its arsenal, which included their nuclear arsenal.[40]

Faced with such difficulties in determining the outcome of the cyber retaliatory attacks and the uncertainties surrounding the reactions of the attacker, nations may choose to forego the option to conduct cyber retaliation. In consequence, this undermines the will to retaliation and compromises the strategy of cyber deterrence.

Overcoming Potential Legal Issues

The current set of international laws can only be applied indirectly to cyber warfare and they are deficient as a legal framework in addressing cyber-attacks.[41] Under international law, it is clear that if Nation A fires a missile at a military base in Nation B, Nation B has the right to defend itself with lethal force. However, it is not so clear if Nation A uses a cyber-attack to cause an explosion at a military base in Nation B, whether Nation B can still exercise its inherent right to self-defence by firing missiles at a military target in Nation A or even launching its own cyber-attack on Nation B.[42]

The legal issues surrounding offensive or retaliatory cyber-attacks are still being widely debated. While there are efforts to define the legal framework for cyber warfare such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* the interpretation of the current set of international laws on cyber warfare differs across various nations. As many of the differences in interpretation stem from the disagreements in key definitions, academics opine that an international treaty or agreement would be necessary to overcome the legal issues on cyber warfare.[43]

As such, maintaining a potentially large library of vulnerabilities could place undue strain on intelligence requirements.

The unclear legal status of cyber warfare and retaliation in the cyber domain presents a challenge in enforcing the will to retaliate. Communicating the will to retaliate or the execution of the cyber retaliation may appear unnecessarily aggressive or even to be contravening international law by some countries. This adds to the pressures faced by the defending nation from amongst the international community.

Involvement of Non State Actors

Cyber-attacks could either be the work of state actors as well as non-state actors. The barrier to entry to carrying out cyber-attacks is low. From a resource perspective, a small group or even an individual can amass enough resources to develop the necessary skills sets and acquire the necessary hardware to carry out cyber-attacks with relative ease.[44] The low barrier of entry was highlighted in a report released by the United States Joint Forces Command in 2010, citing that it would complicate the ability to deter threats.[45]

Blackhat computer groups such as *LulzSec* and *Anonymous* are examples of non-state actors carrying out cyber-attacks, targeting both companies and states.[46] To date, *LulzSec* and *Anonymous* has targeted public websites of US government entities and publicly released stolen data on the Internet.[47]

The involvement of non-state actors in cyber-attacks complicates the strategy of cyber deterrence. These non-state actors may have little worth hitting, thereby raising the question if cyber retaliation is even worthwhile.[48] Even if cyber retaliatory attack is successful in damaging all the computer systems of the non-state attacker, the low barrier to entry would see the attackers be re-equipped quickly.

To make matters worse, if the non-state actor is deliberately shielded and hosted by another country, it may not be legally clear if the state can be even held responsible.[49] Choosing to carry out cyber retaliatory attacks may result in the host country carrying out its own 'cyber retaliation,' pitting the defending nation against both the host country and the non-state actor.

CONCLUSION

Cyber deterrence is a difficult strategy to achieve. The obstacles such as problems in attribution, diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors as well as the potential legal issues, make cyber deterrence an unviable strategy in practice. The risks of misattribution, incurring widespread condemnation and unnecessary escalation would dissuade many nations from adopting this strategy.

The obstacles described in this essay weaken the *will to retaliate* as well as diminish the *capability to retaliate,* both of which are necessary to employ a strategy of cyber deterrence. Adopting a cyber-deterrence strategy is both problematic and risky. Unless new technology allows for speedy attribution to occur or until international norms on cyber-attacks are established, cyber deterrence may remain just an academic construct. In this regard, given today's technology, having a credible and robust cyber defence is the only viable approach.

BIBLIOGRAPHY

Alexander, Keith. US Department of Defence, "Statement Of General Keith B. Alexander Commander United States Cyber Command before the House Committee on Armed Services 23 September 2010."

http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC Command Posture Statement_HASC_22SEP10_FINAL _OMB Approved_.pdf.

Ashford, Warwick. Computer Weekly, "Cyber attack retaliation a bad idea, says international panel."

http://www.computerweekly.com/news/2240206279/Cyber-attack-retaliation-a-bad-idea-says-international-panel.

Campbell, Matthew. *The Sunday Times,* "'Logic bomb' arms race panics Russia."

http://cryptome.org/jya/ru-panic.htm.

Capaccio, Tony. *Bloomberg News,* "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion." April 09, 2009.

http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html

Chng, Grace. *The Straits Times,* "Singapore's cyber defence firepower gets $130m boost." http://www.straitstimes.com/breaking-news/singapore/story/singapores-cyber-defence-firepower-gets-130m-boost-20131026.

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

Egan, Matt. *Fox Business,* "As Cyber Threats Mount, Business is Booming in the Security World."

http://www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/

Fryer-Biggs, Zachery. *Defence News,* "U.S. Military Goes on Cyber Offensive." March 24, 2012.

http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive.

Gartner Inc, . *Infosecurity Magazine,* "Global security spending to hit $86B in 2016." http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016/.

Hathaway, Oona, Rebecca Crootof, and Philip Levitz. "The Law of Cyber Attack." *California Law Review.* n._4 (2012), 826.

http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

Hayley, Christopher. Georgetown Journal of International Affairs, "A Theory of Cyber Deterrence."

http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/.

Hoffman, Stefanie. CRN, "Russian Cyber Attacks Shut Down Georgian Websites." August 12, 2008.

http://www.crn.com/news/security/ 210003057/russian-cyber-attacks-shut-down-georgian-websites.htm.

Kelly, Brian. Boston University Law, "Investing In A Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can And Should Influence Cybersecurity Reform."

http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume92n4/documents/KELLY.pdf.

Kushner, David. IEEE Spectrum, "The Real Story of Stuxnet." December 26, 2013. Accessed February 23, 2014. http://spectrum.ieee.org/telecom/ security/the-real-story-of-stuxnet/.

Lee, Ferran. *ABC News,* "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet."

http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/.

Libicki, Martin. RAND Corporation, "Brandishing Cyberattack Capabilities." Last modified 2013.

http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

LiveSquare Security, "Cyber Warfare: the good, the bad, the ugly."

http://www.arizonatele.com/atic/docs/ATIC_Cyber_Warfare_Presentation_11_17_11.pdf.

Maher, Heather. RFERL, "New Manual Explains Laws Of Cyberwarfare

http://www.rferl.org/content/new-manual-rules-cyberwarfare/24944686.html.

Markoff, John, and David Sanger. The New York Times, "In a Computer Worm, a Possible Biblical Clue."

http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all&_r=0.

Martin Libicki, *Cyberdeterrence and Cyberwarfare,* (Santa Monica: RAND Corporation, 2009), xvi.

Mearsheimer, John. Conventional Deterrence. (Ithaca, New York: Cornell University Press, 1983).

Melzer, Nills. United Nations, "Cyberwarfare and International Law."

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Miller, Greg. *Washington Post,* "FBI director warns of cyberattacks; other security chiefs say terrorism threat has altered."

http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html.

Murchu, Liam. "Stuxnet Using Three Additional Zero-Day Vulnerabilities." Symantec Connect (blog), September 14, 2010. http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

Norton-Taylor, Richard. *The Guardian,* "Britain's Defense Policy Adds Cyber Deterrence to Nuclear Deterrence." September 30, 2013.

http://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence.

Paget, Francis. McAfee Labs, "Hacking Summit Names Nations With Cyberwarfare Capabilities."

http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

Patrick Morgan, *Proceedings of a Workshop on Deterring CyberAttacks:* Informing Strategies and Developing Options for U.S. Policy, (Washington DC: The National Academies Press, 2010), 55-76.

Rehn, Steven. U.S. Army War College, "Don't Touch My Bits or Else! – Cyber Deterrence." http://handle.dtic.mil/100.2/ADA560247.

Robinson Neil, and Walczak Agnieszka, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP),* (Santa Monica: RAND Corporation, 2013), 10.

RSIS, *Effective and Credible Cyber Deterrence,* (Singapore: Centre of Excellence for National Security, 2013).

http://www.rsis.edu.sg/cens/PDF/CENS_Cyber_Security_Workshop_Effective_&_Credible_Cyber_Deterrence.pdf

Secunia, "Time to Patch for All Products," *Vulnerability Security Review* (2014). http://secunia.com/vulnerability-review/time_to_patch.html.

Singer, Peter, and Allan Friedman. Armed Forces Journal, "What about deterrence in an era of cyberwar?"

http://www.armedforcesjournal.com/what-about-deterrence-in-an-era-of-cyberwar/.

Sullivan, Andy. Reuters, "Obama budget makes cybersecurity a growing U.S. priority." Last modified April 11, 2013. http://www.reuters.com/ article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411

Tan, Jeanette. *Yahoo News Singapore,* "Hacker 'The Messiah' claims attack on Singapore govt sites, repeats 'Anonymous' cyber threat." November 05, 2012. http://sg.news.yahoo.com/hacker--the-messiah--claims-attack-on-singapore-govt-sites-repeats-'anonymous'-cyber-threat-090023141.html.

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

UK Parliment, "2 MoD networks, assets and capabilities ."http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm

Waqaas, . Hackread, "Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World."

http://hackread.com/iran-biggest-cyber-army-israel/.

Weisanthal, Joe. *Business Insider,* "Notorious Hacker Group LulzSec Just Announced That It's Finished."

http://www.businessinsider.com/lulzsec-finished-2011-6?IR=T&.

Worstall, Tim. *Forbes*, "Stuxnet Was a Joint US/Israeli Project." http://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/.

ENDNOTES

1. Kushner, David. IEEE Spectrum, "The Real Story of Stuxnet." December 26, 2013. http://spectrum.ieee.org/telecom/ security/the-real-story-of-stuxnet/.

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

   Hoffman, Stefanie. CRN, "Russian Cyber Attacks Shut Down Georgian Websites." August 12, 2008. http://www.crn.com/news/security/ 210003057/russian-cyber-attacks-shut-down-georgian-websites.htm.

3. Tan, Jeanette. *Yahoo News Singapore,* "Hacker 'The Messiah' claims attack on Singapore govt sites, repeats 'Anonymous' cyber threat." November 05, 2012. http://sg.news.yahoo.com/hacker--the-messiah--claims-attack-on-singapore-govt-sites--repeats-'anonymous'-cyber-threat-090023141.html.

4. Capaccio, Tony. *Bloomberg News,* "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion." April 09, 2009. http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.

5. Norton-Taylor, Richard. *The Guardian,* "Britain's Defense Policy Adds Cyber Deterrence to Nuclear Deterrence." September 30, 2013. http://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence

   Fryer-Biggs, Zachery. *Defence News,* "U.S. Military Goes on Cyber Offensive." March 24, 2012. http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive.

6. Hathaway, Oona, Rebecca Crootof, and Philip Levitz. "The Law of Cyber Attack." *California Law Review,* n._4 (2012), 826. http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

7. Murchu, Liam. "Stuxnet Using Three Additional Zero-Day Vulnerabilities." Symantec Connect (blog), September 14, 2010. http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

8. Mearsheimer, John. Conventional Deterrence (Ithaca, New York: Cornell University Press, 1983).

9. Singer, Peter, and Allan Friedman. Armed Forces Journal, "What about deterrence in an era of cyberwar?." http://www.armedforcesjournal.com/what-about-deterrence-in-an-era-of-cyberwar/.

10. RSIS, Effective and Credible Cyber Deterrence, (Singpaore: Centre of Excellence for National Security, 2013). http://www.rsis.edu.sg/cens/PDF/CENS_Cyber_Security_Workshop_Effective_&_Credible_Cyber_Deterrence.pdf

11. Hayley, Christopher. *Georgetown Journal of International Affairs,* "A Theory of Cyber Deterrence." http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/.

12. Ibid.

13. UK Parliment, "2 MoD networks, assets and capabilities." http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm.

14. Martin Libicki, *Cyberdeterrence and Cyberwarfare,* (Santa Monica: RAND Corporation, 2009), xvi.

15. Ibid., 73.

16. Rehn, Steven. U.S. Army War College, "Don't Touch My Bits or Else! – Cyber Deterrence." http://handle.dtic.mil/100.2/ADA560247.

17. Patrick Morgan, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy,* (Washington DC: The National Academies Press, 2010), 55-76.

    RSIS, *Effective and Credible Cyber Deterrence,* (Singapore: Centre of Excellence for National Security, 2013). http://www.rsis.edu.sg/cens/PDF/CENS_Cyber_Security_Workshop_Effective_&_Credible_Cyber_Deterrence.pdf

18. Ibid., 16, 32.

19. Gartner Inc, . Infosecurity Magazine, "Global security spending to hit $86B in 2016." http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016/.

20. Ibid., 5, 12.

21. Egan, Matt. *Fox Business,* "As Cyber Threats Mount, Business is Booming in the Security World." http://www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/.

22. Sullivan, Andy. Reuters, "Obama budget makes cybersecurity a growing U.S. priority." http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411.

23. Miller, Greg. Washington Post, "FBI director warns of cyberattacks; other security chiefs say terrorism threat has altered." http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html.

24. Chng, Grace. *The Straits Times,* "Singapore's cyber defence firepower gets $130m boost." http://www.straitstimes.com/breaking-news/singapore/story/singapores-cyber-defence-firepower-gets-130m-boost-20131026.

25. Paget, Francis. McAfee Labs, "Hacking Summit Names Nations With Cyberwarfare Capabilities." http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

26. Robinson Neil, and Walczak Agnieszka, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*, (Santa Monica: RAND Corporation, 2013), 10.

27. Waqaas, . Hackread, "Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World." http://hackread.com/iran-biggest-cyber-army-israel/.

28. Alexander, Keith. US Department of Defence, "Statement Of General Keith B. Alexander Commander United States Cyber Command before the House Committee on Armed Services 23 September 2010." http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC Command Posture Statement_HASC_22SEP10_FINAL _OMB Approved_.pdf.

29. Worstall, Tim. *Forbes,* "Stuxnet Was a Joint US/ Israeli Project." http://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/.

30. Markoff, John, and David Sanger. *The New York Times,* "In a Computer Worm, a Possible Biblical Clue." http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all&_r=0.

31. Lee, Ferran. *ABC News,* "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet." Last modified July 09, 2013. Accessed March 3, 2014. http://abcnews.go.com/ blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/.

32. Ashford, Warwick. *Computer Weekly,* "Cyber attack retaliation a bad idea, says international panel." http://www.computerweekly.com/news/2240206279/Cyber-attack-retaliation-a-bad-idea-says-international-panel.

33. Ibid., 16, 43.

34. Ibid., 16, 41.

35. Secunia, "Time to Patch for All Products - *Vulnerability Security Review* (2014) http://secunia.com/vulnerability-review/time_to_patch.html.

36. Libicki, Martin. RAND Corporation, "Brandishing Cyberattack Capabilities." http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

37. Ibid., 27.

38. Ibid., 16, 58.

39. Ibid., 16, 69.

40. Campbell, Matthew. *The Sunday Times,* "'Logic bomb' arms race panics Russia." http://cryptome.org/jya/ru-panic.htm.

41. Ibid., 8.

42. Maher, Heather. RFERL, "New Manual Explains Laws Of Cyberwarfare." http://www.rferl.org/content/new-manual-rules-cyberwarfare/24944686.html.

43. Melzer, Nills. United Nations, "Cyberwarfare and International Law." http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

44. LiveSquare Security, "Cyber Warfare: the good, the bad, the ugly." http://www.arizonatele.com/atic/docs/ATIC_Cyber_Warfare _Presentation_11_17_11.pdf.

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

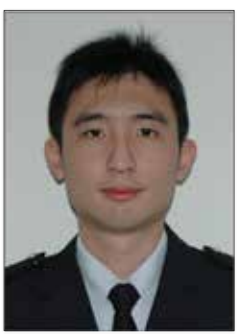
46. Weisanthal, Joe. Business Insider, "Notorious Hacker Group LulzSec Just Announced That It's Finished." http://www.businessinsider.com/lulzsec-finished-2011-6?IR=T&.

Kelly, Brian. Boston University Law, "Investing In A Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can And Should Influence Cybersecurity Reform." http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume92n4/documents/KELLY.pdf.

47. Ibid., 46.

48. Ibid., 16, 70.

49. Ibid., 16, 58.



MAJ Lee Hsiang Wei is currently a Senior Policy Officer in the Defence Policy Office, MINDEF HQ. A Helicopter Pilot by vocation, MAJ Lee was previously an operational pilot in 126 SQN. MAJ Lee was a recipient of the SAF Overseas Scholarship in 2004 and graduated from Cornell University with a Masters of Engineering and a Bachelors of Science in Electrical and Computer Engineering. MAJ Lee also won the 2nd prize in the annual Chief of Defence Force Essay Competition in both 2012 and 2014.

Armed Forces and Societies: Implications for the SAF

by **CPT Ren Jinfeng**

Abstract:

The increasing professionalisation of the armed forces is a challenge to a nation's defence strategies and the armed forces is forced to adapt to socio-political changes, resulting in increasing inter-penetrability of civilian and military spheres and cultures. As such, the military has to constantly review its structural relationship with society and strategic roles to anchor its legitimacy. Therefore, the SAF must continue to engage the larger civil society in defence policy issues, to encourage a greater sense of co-ownership and to sustain efforts in increasing the 'social capital' for the SAF. This essay examines the historical overview of the armed forces in societies, the decline of conscription army during the post-Cold War period and the dominant trend in modern armed forces, as they adapt their roles, to strengthen the linkage to and the legitimacy in the society. This essay also studies the implications of such trends for the SAF.

Keywords: Defence Strategies, Modern Armed Forces, Implications, Socio-Political Circumstances

INTRODUCTION

In the post-Cold War order, many states are struggling to ensure the legitimacy, relevance and connection between their armed forces and societies. Most of the armed forces have shrunk significantly as compared to their pre-Cold War force size, partly because of the end of the conscription system and a shift towards a volunteer professional army.[1] Significantly, this has removed a major mechanism through which the armed forces and their respective societies interact with each other. In many states, the military budgets have also shrunk as the governments reprioritise their budget allocation amidst changing socio-economic circumstances. In response to these trends, the armed forces are forced to adapt their structures and policies, resulting in an increasing inter-penetrability of civilian and military spheres and cultures.[2] At the same time, the roles of the armed forces continue to evolve, as they strive to enhance their bases for legitimacy.

This essay will begin with a historical overview of the armed forces in societies, particularly on the rise and fall of the mass army or the conscription system in nation-states. The essay will then closely examine the factors leading to the decline in the mass army in the post-Cold War nation-states and explore the dominant trend in modern armed forces as they adapt their roles to strengthen the linkage to and legitimacy in the society. Lastly, the essay will examine the implications of such trends for the Singapore Armed Forces (SAF).

HISTORICAL OVERVIEW OF ARMED FORCES IN SOCIETIES

All modern nation-states organise and mobilise their people to serve in the military. The modalities through which the states mobilise and institutionalise its defence have direct impact on their prospects to win wars and ensure survival, the military options available for the conduct of foreign affairs with a high degree of freedom and the degree of integration between the military and the society.[3] In modern history, the western world witnessed the rise of the mass armed forces as a major form of military mobilisation since the 18th century and its rapid decline in the post-Cold War order. An understanding of the factors leading

to the ebb and flow of the conscription system in these societies is therefore necessary, not least for predicting its long-term viability in modern societies.

Till the 18th century, the armies in Europe mostly adopted an aristocratic model in which militaries were raised in defence of the crown.[4] The armed forces were led by members of the noble class, so as to ensure integrity with the political elites and continuity of rule over the commoners. Entrusting arms to the hands of the subjects was unheard of, as the rulers were fearful that such a practice would have egalitarian consequences and thus undermine their rule.[5]

Towards the end of the 18th century, this predominant model of military mobilisation was challenged by the emergence of the mass armed forces, brought about by the democratic revolutions in America and France. As part of the Revolution, the French decreed the *levee en masse* in 1793, aiming to mobilise the entire French nation through compulsory military service.[6] It should be noted that the shift from the aristocratic model to the mass mobilisation of citizens was no less than a radical move that was reluctantly accepted by the rulers out of necessity. Indeed, it did not immediately triumph over the aristocratic model. Widespread adoption of the mass armed forces through compulsory military service did not happen till the late 19th century. During this period, most European countries returned to the aristocratic model, including France. It was not until the Prussian army fundamentally reformed their military after their defeat against the Poles and Danes, adopted mass mobilisation and secured their victories, that conscript-based armies became the standard model for mobilising manpower for wars in Europe till the end of World War II (WWII).

In sum, the mass armed forces were raised out of necessity perceived by the states and/or their people, under favourable socio-political circumstances.

It would be simplistic or naïve to think that the conscription system was only borne out of the new democratic ideology during the Revolutions. Undeniably, as some military sociologists argued, the birth of conscription could be attributed to fundamental ideological shifts—the conception of a 'citizen-soldier as an individual ideal and of the nation as a nation in arms' and mobilising people for war.[7] However, such an ideological change was insufficient to explain the radical change, as evident in the fact that the military service was compelled, illustrating that nationalistic and patriotic sentiments alone were inadequate. First and foremost, the states and/or their people had to recognise the need for mass conscription. The concept of the

Cyberpioneer

NSmen from 694 SIR and 695 SIR marching off at the parade, having fulfilled their service to the nation.

mass army was conceived and accepted as a radical change by the rulers in the 18th century because the states were drawn into wars that threatened the very survival of the states, so much so that the political elites were willing to convert their subjects into citizens of the nation-state, thereby involving them in national politics. To further illustrate, both the United Kingdom (UK) and the United States (US) did not adopt mass conscription till World War I (WWI), when they were compelled to do so. However, they immediately abolished the system after WWII. Secondly, the concept of war in the earlier centuries was centred on mass-on-mass attrition. Mass conscription then ensured military sustainability, while "clothed in the ideology of democracy."[8] In addition, a few other socio-economic factors were essential for the transformation. These included increase in population size and wealth, a surplus of unemployed young men and spread of literacy. In sum, the mass armed forces were raised out of necessity perceived by the states and/or their people, under favourable socio-political circumstances.

The fundamental driving force for this trend of increasing professionalisation of the armed forces was a drastic shift in geopolitical threat environment and hence changing the nation-states' defence strategies.

POST-COLD WAR DECLINE IN MASS ARMY: CONSCRIPTION CRISIS?

The Decline of Mass Armed Forces

After WWII, the western world saw a rapid decline in their reliance on mass conscription as the model to mobilise their people for defence and a concomitant shift towards all-volunteer professional force. By the 1970s, both the UK and the US had abolished the system, while the most of the European countries saw their reliance on conscript-based armed force fall, as reflected in the reduction in conscript ratio, i.e. the proportion of conscripts to the regular force. Between 1961 and 1986, the average duration of the compulsory military service in European countries dropped from 18 months to 12 months.[9] The end of the Cold War accelerated this trend. Between 1970 and 2000, there was universal conscription in all 15 analysed European nations (less Great Britain).[10] After 1991, the majority of these nations ended their conscription, except a few countries such as Finland, Turkey and Switzerland. The military participation ratio, a measure of the share of a country's population enrolled in the military, also decreased from an average of 3% to 5% during this period.[11] Notably, for countries that still retained the conscription system, the conscript ratio decreased further. In addition, these nations continued to face increasing budgetary constraints.

The fundamental driving force for this trend of increasing professionalisation of the armed forces was a drastic shift in geopolitical threat environment and hence changing the nation-states' defence strategies.[12] In the bipolar world order during the Cold War, Western Europe faced a common threat, with their defence strategy anchored on nuclear deterrence. The breakdown of the world order, exacerbated by the post-9/11 threat environment, created a huge socio-political pressure for the military to reform and restructure in facing new geopolitical challenges. At the same time, nations found themselves having to deal with an expanded mission scope beyond

Platoon Commander Lieutenant (LTA) Vivien Lee (far left) introducing the Singapore-version of the Leopard 2SG MBT to troops from the German army's 33rd Panzer battalion.

President Tony Tan Keng Yam inspecting the Officer Cadet contingents at the 95th Officer Cadet Course Commissioning Parade held at SAFTI Military Institute.

conventional warfighting to include international security missions. The reduced resources available, coupled with expanded mission demands, created a growing expectation-capability gap in the armed forces and drove fundamental reforms within the military towards professionalisation. The degree of professionalisation and the eventual institutional arrangement of the military depend on the socio-political environment and the new defence policy objectives for their militaries. These resulted in generally four models of armed forces in post-Cold War Europe focusing on Expeditionary Warfare (full spectrum of operations), Territorial Defence (low to medium spectrum of conflict), Late Modern (limited capacity to cover full range) and Post-Neutral (low intensity operations).[13]

Outside Europe, nations witnessed similar trends towards a removal or reduction in conscription, although the contributing factors might vary significantly from those in Europe. Notably, some of these nations continue to face mounting unpopularity towards compulsory national service, even though they face relatively more immediate threats. In Taiwan, the conscript period has been reduced steadily over the years, in spite of China's continued threat to resort to military action to regain sovereignty over Taiwan. Recently, the Taiwanese government announced an eventual abolishment of the conscript system by 2017, delayed from the initial timeline of 2015.[14] The delay occurred after a mass protest over the death of a serviceman due to physical punishment in camp and difficulties in recruiting enough regular personnel.[15] In South Korea, the conscript system attracted scathing criticism as a result of growing intolerance towards inequality in the system, whereby the powerful and the rich found ways to evade conscription.[16] A 2014 survey showed that 68% agreed with the adoption of alternative civilian service, as compared to 44.3% in 2008.[17]

This trend of a decline of conscription system in societies, be it a total removal of the system or a shift towards greater professionalisation through the hiring of more regular personnel, are consequential in at least three significant ways.[18] First, it has direct impact on the deterrence posture of the nation. It significantly reduces the nation-state's ability to win conflicts as the overall force size and quality of the troops decrease. This is particularly true for relatively small armed forces. Second, it affects the capacity of the nation to conduct its foreign affairs with a high degree of freedom, as the latter pre-supposes the viability and range of military options available, which in turn, depend partly on the force structure. Third, it affects the way the military influences and is influenced by the society which it aims to protect. As articulated by Janowitz,[19] effective citizenship and integration with society must be cultivated through participatory civic engagement; and when being a citizen-soldier is no longer a shared experience in the society, the nation loses one of the most effective means of civic engagement—something strongly echoed by the first Singapore Defence Minister, Dr. Goh Keng Swee. In his parliamentary speech on National Service, Dr Goh envisioned that "there is another aspect to our defence efforts. This is a contribution it can make to nation building. Nothing creates loyalty and national consciousness more speedily and thoroughly than participation in defence and membership of the armed forces."[20]

Explaining the Decline

Given the significant impact the removal or reduction of conscription could have on the societies, the various factors leading to the global trend warrant close examination. This essay would focus on the socio-political factors, rather than other contributory factors such as strategic shifts from nuclear deterrence in post-Cold War order and the impact of technological advancement on military reforms, although these factors are no less significant.

One of the most significant factors is the disappearance of threat, perceived or not.[21] In the context of Europe, the effects of post-Cold War geopolitical reality were far-reaching. The general populace believed that major conflicts were far removed from the heart of the continent. For instance, a 1996 survey conducted in Paris revealed a shift of threat perception to mainly around 'terrorism, pollution and drugs'. As a consequence, Europe in the 1990's underwent a period where there was no consensus on the priorities of the military and was considered of secondary importance. Mass conscription was removed in many nations. Military budgets shrank significantly, as much as 30-50% in some countries.[22] Even the post-9/11 environment did little in reversing the trend. Similarly in Taiwan, some argued that the warming ties with China in recent years could have contributed towards some public perception that there was no immediate threat of invasion.[23] Also related to this factor is the shift in mission from territorial defence to international peacekeeping and security. This has led to new military policy thinking that conscripted armed forces are no longer suited for these new mission types.[24]

However, threat perception alone is insufficient to guarantee a sustained public support towards the military or conscription. The perceived effectiveness of the military in fulfilling its purpose and in defending the interests of the nation plays an equally important role. In Taiwan, there is widespread public opinion that the People's Liberation Army of China has grown so powerful relative to the armed forces in Taiwan that any attempt of resistance would be futile.[25] In countries such as Ukraine, low levels of investment in military equipment and infrastructure and military ineptitude in combat had led to almost a "near complete collapse in societal legitimacy."[26]

The third factor is the fundamental change in the socio-political landscape within society. Increasing affluence and education have been cited as a common trend and reason for the military reforms within nations.[27] This goes hand in hand with a structural shift in the society, whereby nations find it increasingly difficult to centrally

organise and mobilise the populace.[28] This is further accompanied by a cultural shift, in which there is widespread decline in public deference to authority and an 'attenuation of nationalistic sentiments' that legitimised compulsory military service during the early days of the nation-states.[29] However, it should be pointed out that research data has revealed that the link between increasing living standards of a society and the corresponding decline in conscription is not the most significant factor. Notably, Switzerland has the highest GDP per capita in the European countries studied and yet also has the highest Conscript Ratio.[30] The effects of waning threat perception, being part of a larger military alliance such as NATO and shift in core mission to international security missions were cited as the more significant driving forces.[31]

Against this societal backdrop, a lack of equity or universality in the implementation of conscription will further erode public support significantly. In South Korea, there has been persistent public discontent towards the irregularities in the system whereby the rich and the influential found means to evade duty, as exposed by the media throughout the 1990's and early 2000's.[32] The complex conscription system entails different lengths of service and remunerations for different servicemen. Such inconsistency has been a constant source of public unhappiness. In Israel, the exemption of the Ultra-orthodox community from national service has also been a persistent source of discontent amongst those who serve.[33] While the Israeli government recently passed a law to remove the exemption, the long-term impact and viability are less certain given the strong reaction from the Ultra-orthodox community.[34]

Lastly, the media has played a crucial role in shaping public opinions about the military. This took place when the media was divorced from the military, which used to be embedded within and greatly controlled by the military during the two World Wars.[35] The increasing autonomy of media, enabled by technological advancement in media transmission, has fundamentally changed the way the public receives and expresses opinions towards the military. A good illustration was the exposure by media on the series of scandals involving the powerful and influential leaders in South Korea who evaded compulsory military service.

MILITARY ROLES AND LEGITIMACY

Today, military forces around the world continue to be shaped by these socio-political changes. Against this trend of decline in mass armed forces and towards increasing professionalisation, the militaries in these societies have strived to review both their structural relationship with their society and their strategic roles, in an attempt to consolidate their legitimacy.

Indeed, it has been recognised that the armed forces are institutionalised for a range of purposes, beyond its tradition core mission of territorial defence.[36] While the military is often centred on the use of organised violence in territorial defence of the nation, the utility of the armed forces continues to be shaped and reshaped by both social and political demands and expectations. Forster identified five functional roles played by the military, which determine its legitimacy and relationship with the society.[37] These include:

(a) National Security - the definition of which has broadened beyond territorial defence. It is deemed as the core source of legitimacy for the militaries, particularly in nations where threat is widely perceived and accepted. However, it is noted that 'such "representations of danger" are not "given" but are socially and politically constructed.'[38]

(b) Nation Building - Perceived as closely related to the role of National Security and will enhance the military's legitimacy through the promotion of national values and identity.

(c) Regime Defence - Often found in authoritarian regimes.

(d) Domestic Military Assistance – Here, the legitimacy gained will depend on not only the demand on the armed forces, but also on the effectiveness of the armed forces in fulfilling such tasks.

(e) Military Diplomacy – The way which the military is used to pursue and enlarge the political and foreign policy space.

The permutation and priorities of these roles adopted by the military often determine the ability of the military to renew and enhance its legitimacy. Forster further identified three types of civil-military relationships, based on the evolving bases for legitimacy.[39] In the Ossified Legitimacy group, countries such as Ukraine and even Switzerland are losing legitimacy based on their old, outdated rationale for the armed forces, while having failed in promoting new roles and relevance. This has often led to rising difficulties in recruiting and retaining personnel in the military. In the re-connected Legitimacy group, countries such as Poland and Denmark successfully adapted new roles to sustain their position in the society. With the end of the Cold War, public support for the military increasingly declined. Following a re-strategising by the government in 1992, the armed forces had increasingly developed an international security mission beyond their national territory. This managed to reverse the public support trend in Denmark. In the last category of Renewed Military, the armed forces continued to strengthen public opinions through the introduction of new roles. In the case of Italy, its continued roles in National Building, and more recently in international missions, have bolstered the public support for their armed forces.

IMPLICATIONS FOR THE SAF

This global trend in the military conscription system in other nation-states is instructive for the SAF, as it continues to strengthen public support for the National Service (NS) system. Today, the public sentiments towards NS are positive, as more than 98% regarded NS as the "cornerstone for the security and prosperity of Singapore."[40] However, signs are emerging

ACCORD members, with Dr Maliki (second from right), listening to a briefing by the Commanding Officer of 191 Squadron, Colonel Thng Chee Meng (second from left) on the flight deck of RSS Endurance at the SAF50@VIVO event on 14th February 2015.

over the horizon that warrants attention, as indicated by alternative opinions that the conscription system should be re-considered.[41]

First, there is a continued need to balance between shaping threat perception and both the larger defence policy and operational security considerations, which tend to minimise public awareness of tensions with the neighbouring countries. This could be seen from the effects of waning threat perception on the European countries and their conscription systems, and to some extent, also in the context of Taiwan. Recent diplomatic spats such as the naming of the Indonesian ship after Usman and Harun are timely reminders, but the impact on the public memory is likely going to be short-lived. With changing demographics and greater proportion of the population being born in post-Konfrontasi period, there is greater imperative to convince the public on the need for a strong SAF in defending the interests of the nation.

Against a changing domestic socio-political landscape, where there has been a fundamental cultural shift in public opinions, the SAF should also continue to engage the larger civil society in defence policy issues and to encourage a greater sense of co-ownership where appropriate.

However, as illustrated in the recent Crimea crisis and also in the context of Taiwan, the existence of threat alone is inadequate in garnering strong support for the military institution, should the latter fail to demonstrate its effectiveness in fulfilling its core mission of defence. To this end, the SAF has successfully undergone a decade of transformation and it should continue to do so, to instil strong public confidence in the SAF as the guarantor of Singapore's sovereignty.

Against a changing domestic socio-political landscape, where there has been a fundamental cultural shift in public opinions, the SAF should also continue to engage the larger civil society in defence policy issues and to encourage a greater sense of co-ownership where appropriate. In this light, the Committee to Strengthen National Service has made significant strides, in ensuring that public feedback are diligently considered and re-worked into NS policies. Indeed, there is a need for sustained efforts in increasing the 'social capital' for the SAF,[42] so that public support remains strong in view of the changing demographics and uncertainties ahead. However, the changing social landscape also spells a greater need to uphold the principle of universality for conscription—a lesson to be learned from countries such as South Korea and Israel. In this light, there is a need to continue reviewing the conscription policy for immigrants and new citizens, as voiced consistently in the recent years,[43] albeit being a contentious and controversial issue. In this sense, the recent announcement to encourage the first-generation Permanent Residents to volunteer in the military should be viewed in a positive light.

In addition, it should be noted that the functional roles of the military remain dynamic, as the military evolves to meet societal expectations and enhance its legitimacy. As such, the recent survey conducted by the Institute of Public Policy pointed out that the view that Singaporeans considered 'instilling discipline and values among the young' as slightly more significant than 'for National Defence' should not be taken too pessimistically.[44] Instead, this should be viewed together with the overall consensus that NS remains relevant and important in the public mind. Going forward, we should be mindful that the perceived roles of the military are dynamic and not static in the public mindshare. More critically, the SAF should continue to adapt and adopt a more relevant and engaging narrative to anchor its legitimacy in society.

CONCLUSION

Over the past few centuries, the world witnessed the rise and fall of the mass armed forces as the dominant format of institutionalised military mobilisation in the societies. While the contributory factors are many, including changing nature of warfare and technological advancement, analysis points to socio-political factors as significant drivers that explain the continued decline of conscription in societies. Against this backdrop, militaries have attempted to review their roles and to renew their legitimacy within societies. The ability of the military to adapt determines its ability to stay relevant in the public mindshare. Consequently, this has significant impact on the nations' defence, foreign policy and civil-military relationships. These trends and driving factors, are instructive for the SAF, as it continues to build upon its strong foundation in anchoring public support.

ENDNOTES

1. Forster, Anthony, *Armed Forces and Society in Europe,* (London: Palgrave Macmillan, 2006), 97.
2. Wilfried von Bredow, "Conceptual Insecurity, New war, MOOTW, CRO, Terrorism and the Military", *Social Sciences and the Military: An Interdisciplinary Overview,* (Cass Military Studies, 2007), 174.
3. Burk, James, "Military Mobilisation in Modern Western Societies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 111
4. Ibid., 112.
5. Ibid., 112.
6. Burk, James, "Military Mobilisation in Modern Western Societies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 113
7. Ibid., 113.
8. Ibid., 116.
9. Ibid., 118.
10. Haltiner, Karl, "The Decline of the European Mass Armies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 367. These countries include Netherlands, Belgium, Portugal, France, Denmark, Spain, Germany, Italy, Austria, Norway, Greece, Sweden, Finland, Turkey and Switzerland.
11. Ibid., 368.
12. Forster, Anthony, *Armed Forces and Society in Europe,* (London: Palgrave Macmillan, 2006), 41.
13. Ibid., 45.
14. Mishkin, Sarah, "Taiwan Prepares for End of Conscription", http://www.ft.com/cms/s/0/489ed4c4-1eaa-11e2-bebc-00144feabdc0.html#axzz2xRG5k61j
15. Chris Wang, "Date for All-Volunteer Military Delayed", http://www.taipeitimes.com/News/front/archives/2013/09/13/2003572014
16. Young-key Kim-Renaud, "The Military and South Korea Society", https://www.gwu.edu/~sigur/assets/docs/scap/SCAP26-HMS05.pdf
17. Strother, Jason, "In South Korea, A Student Battles Against Compulsory Military Service", http://online.wsj.com/news/articles/SB10001424052702304302704579331583743130494
18. Burk, James, "Military Mobilisation in Modern Western Societies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 111.
19. Burk, James, "Military Mobilisation in Modern Western Societies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 125.
20. Goh Keng Swee, http://www.nas.gov.sg/1stcab/PanelPDF/Section%202%20-%20Defending2.pdf
21. Boene, Bernard, "The Military As a Tribe Among Tribes", *The Handbook of Sociology of Military,* (Dordrecht: Kluwer Academic, 2003), 172.
22. Ibid., 172.
23. Cole, Michael, "Taiwan's Volunteer Military: Vision or Nightmare" http://thediplomat.com/2013/07/taiwans-all-volunteer-military-vision-or-nightmare/

24. Caforio, Giuseppe, "Trends and Evolution in the Military Profession", *Social Sciences and the Military: An Interdisciplinary Overview,* (Cass Military Studies, 2007), 218.

25. Cole, Michael, "Taiwan's Volunteer Military: Vision or Nightmare", http://thediplomat.com/2013/07/taiwans-all-volunteer-military-vision-or-nightmare/

26. Forster, Anthony, *Armed Forces and Society in Europe,* (London: Palgrave Macmillan, 2006), 84.

27. Burk, James, "Military Mobilisation in Modern Western Societies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 125.

28. Moskos, Charles, "Towards Postmodern Military?", *Democratic Societies and Their Armed Forces:Israel In Comparative Context,* (Frank Cass, 2000), 4.

29. Burk, James, "Military Mobilisation in Modern Western Societies", *Handbook of the Sociology of the Military,* (Kluwer Academic, 2003), 125.

30. Haltiner, Karl, "The Decline of the European Mass Armies", *Handbook of the Sociology of the Military,* (Dordrecht: Kluwer Academic, 2003), 361.

31. Ibid., 377.

32. Young-key Kim-Renaud, "The Military and South Korea Society", https://www.gwu.edu/~sigur/assets/docs/scap/SCAP26-HMS05.pdf

33. Kasnett, Israel, "A View From Israel: Conscription Now", http://www.jpost.com/Opinion/Columnists/A-View-from-Israel-Conscription-Now

34. "Orthodox Jews Outraged as Israel Passes Military Conscription Law', http://rt.com/news/jews-israel-law-military-354/

35. Forster, Anthony, *Armed Forces and Society in Europe,* (London: Palgrave Macmillan, 2006), 220

36. Ibid., 75.

37. Ibid., 73-98.

38. Campbell, 1992, as cited in Forster, Anthony, *Armed Forces and Society in Europe,* (London: Palgrave Macmillan, 2006), 77

39. Forster, Anthony, *Armed Forces and Society in Europe,* (London: Palgrave Macmillan, 2006), 81

40. Leong, et al, "Singaporeans' Attitude to National Service", Institute of Policy Study, LKY School of Public Policy, National University of Singapore (2013).

41. Kirsten Han, "Is It Time to Reconsider National Service?", https://sg.news.yahoo.com/blogs/singaporescene/time-reconsider-national-233656851.html

    Zach Isaiah Chia, "A Different Defence Model", http://theindependent.sg/ns-debate-part-1-a-different-defence-model/

42. Ulrich vom Hagen, "Social Capital: The Currency of the Armed Forces", *Challenge and Change for the Military,* (McGill-Queen's University Press, 2004), 74

43. Lim, Alvin, "On Alex Liang, a Singaporean who gave up his Singapore Citizenship", http://alvinology.com/2013/10/04/on-alex-liang-a-singaporean-who-gave-up-his-singapore citizenship/

44. Leong, et al, "Singaporeans' Attitude to National Service", Institute of Policy Study, LKY School of Public Policy, National University of Singapore (2013).

CPT Ren Jinfeng is a UAV Pilot - IO (Air Int) by vocation. He is currently the Staff Assistant to the Chief of Air Force. He graduated with a Bachelors of Engineering in Materials Science and Engineering from the Imperial College London in 2009 and a Masters of Engineering in Materials Science and Engineering from the Massachusetts Institute of Technology in 2010.

Hype or Reality: Putting the Threat of Cyber Attacks in Perspective

by **CPT Lim Ming Liang**

Abstract:

The potential threat of cyber-attacks has been a subject of concern for military and national security. Especially in the United States, cyber threat is deemed as a crucial problem that could compromise the security of a nation and is regarded as 'acts of war'. There have been known cases of attacks against religious corporate and government groups—formed by non-state cyber groups—and this has further escalated the need for cyber security. The essay also highlighted various findings that question the plausibility for cyber-attacks to compromise national security. This essay will address the levels and measures of cyber threats, its limitations and the strategies against it, as well as instances of cyber-attacks that were being used against states. It will also address the extent of the damage cyber threats can bring and the viability of its impact on national security.

Keywords: Military and National Security, Technology, State Secrets, Impact

INTRODUCTION: CYBER ATTACKS IN POLITICAL AND ACADEMIC DISCOURSE

In 2011, the former United States (US) Secretary of Defence warned the American Senate that "the next Pearl Harbour could very well be a cyber-attack."[1] The language, coupled with the speaker's identity and a budget-approving audience bodes of securitisation.[2] It is, however, beyond the object of this essay to scrutinise why politicising the cyber threat is in the interest of the US Department of Defence and its military. Expectedly, America's securitising of the cyber threat has evoked similar fears among various states as national cyber commands begin to emerge in other technologically-advanced countries. At the same time, non-state cyber groups such as Anonymous, which is notable for high-profile hacks and denial-of-service (DOS) attacks against religious, corporate and governmental groups and the Syrian Electronic Army which consists of hackers supporting Syrian President Bashar al-Assad, are also active in cyberspace. Even more worrisome is the Pentagon's announcement in 2011 that it will categorise hostile acts in cyberspace as acts of war and that the US reserves the right to retaliate with all necessary means, including a nuclear response.[3] This landmark discourse has essentially opened the floodgate for militarising and escalating attacks in the cyber domain.

US Navy Cyber Defense Operations Command Monitor

The hype of cyber security in the political arena is supported with analyses from the security studies academia. A group of scholars advance the cyber revolution thesis which claims that cyber-

attacks present a perilous threat to states. Most of these works identify cyber-attacks as possible of being independent of traditional military systems, inherent with the problem of attribution which conceals its perpetrators, having an asymmetric nature with low entry of barriers, hence favouring weak states & non-state actors; and imposing a zero-sum paradox on technologically-advanced states as they are concurrently more vulnerable.[4] Others purport that current cyber operations are primarily offence-dominant and that a serious cyber-attack can bring about catastrophic destruction.[5] In sum, the cyber revolution theorists affirm the securitisation of cyberspace and advance that cyber-attacks revolutionalise warfare and impose an unprecedented vulnerability on states.

Herein, any attempt that aims or results in the direct compromise of the state's monopoly of force within its national borders or diminishes its ability to preserve its territorial integrity constitutes a threat to a state's security.

Against this backdrop, the virtual peril of the cyber domain is palpable. How secure are states in the advent of widespread cyber-attacks and the rise of both state and non-state cyber groups? Do cyber-attacks really threaten our nation's security? This essay seeks to put the threat of cyber-attacks in perspective and provide an objective answer to the question in the following manner. Firstly, it presents an empirical study of recent cyber-attacks to objectively assess their existing trend and risk profile. This takes the form of a risk assessment and bubble chart plot of recent cyber-attacks based on their threat level, likelihood and frequency. Secondly, it conducts a short case study on two significant cases of cyber-attacks to complement the empirical study. Thirdly, it aggregates the findings of the previous two sections to contest the cyber revolution thesis. Finally, this essay also proposes principles for a tenable cyber strategy. In so doing, it will argue that the cyber threat is overrated and that current cyber-attacks do not yet threaten states' security.

At this point, it is useful to specify the definitions of the state and its security for an objective discussion to avoid conflating the concept of security. Max Weber inspired a means-centric understanding of a state that state theorists described as having born of medieval war-making or "war made the state and the state made war."[6] Christopher Pierson added that the state's central activity of war-making is 'turning outwards' to achieve the ends of defending the state's territorial integrity and its monopoly of (legitimate) force for social order within its territory.[7] According to Pierson, these ends are one of the primary goods that the modern state provides for its citizens, requisite among a host of other economic and social goods. Any discussion of security necessitates first, an identification of its referent object and second, the values that the referent object seeks to be free from threat.[8] In this case, the state is the referent object which desires to maintain a "low probability of damage" to its values of territorial integrity and monopoly of legitimate force.[9] These are plausible definitions that policy-makers and scholars in the security arena can identify with.

Herein, any attempt that aims or results in the direct compromise of the state's monopoly of force within its national borders or diminishes its ability to preserve its territorial integrity constitutes a threat to a state's security. In this spirit, a foreign cyber-attack that disables or damages a squadron of a state's air force remotely, for example, is considered to have threatened the security of said state as its monopoly of force within its territory has been diminished.

RISK PROFILE OF RECENT CYBER ATTACKS

In the face of a burgeoning discourse on the dangers of cyber-attacks, an empirical study of these attacks presents an objective approach to discern between hype and reality. The Centre for Strategic and International Studies (CSIS) list of "Significant Cyber

Threat \ Likelihood				
Moderate Risk	Moderate Risk	High Risk	High Risk	High Risk
Moderate Risk	Moderate Risk	Moderate Risk	High Risk	High Risk
Low Risk	Low Risk	Moderate Risk	Moderate Risk	High Risk
Low Risk	Low Risk	Low Risk	Moderate Risk	Moderate Risk
Low Risk	Low Risk	Low Risk	Low Risk	Moderate Risk

Table 1: 5x5 Risk Assessment Matrix

Incidents Since 2006" recorded 153 cases of high profile attacks on government agencies, defence and technology companies as well as economic crimes with losses of more than a million dollars.[10] Of these, 90 out of the 153 incidents targeted government agencies. This study will exclude the other 63 cases of civil and corporate cybercrime and attacks which is consistent with the definition of security proposed earlier.

Methodology

In this study, each of these cases will be coded with a 'threat' and a 'likelihood' score. These factors are functions of a simplified risk equation (Risk = Threat x Likelihood), as other information such as vulnerability is unavailable.[11] This formula produces a risk assessment 5x5 matrix that can reasonably determine risk. *Table 1* shows the matrix that the study uses with each cell colour-coded with red, yellow or green to indicate the respective level of risk – high, moderate or low.[12]

For each of the incidents in the CSIS List, the 'threat' score is ordinally measured on a five-point scale which determines the consequential severity of an attack where a score of 'one' denotes the types of attack with the least impact and a score of 'five' denotes a cyber-war with catastrophic consequences. The five-threat levels and their corresponding type of attack and description are summarised in *Table 2*. 'Likelihood' operationalises the sophistication required and scale of the cyber-attack on a five-point ordinate measure where a score of 'one' denotes a high-technology and high-cost, usually state driven effort while a score of 'five' denotes a low cost and easily

Score / Type of Attacks	Threat Description
1 Disruption	Cyber penetration, or disabling of systems (including denial-of-service attacks)
2 Subversion	Penetration with modifications or vandalism of websites to undermine or challenge authority or society (including hacktivism)
3 Espionage	Penetration for purposes of extracting sensitive or protected information
4 Sabotage	Penetration leading to physical damage, malfunction or destruction of critical systems or infrastructure
5 Cyber War	Loss of lives and infrastructure as a result of cyber attacks

Table 2: Ordinate Measurement for Threat

Score	Likelihood Description
1 Least Likely	When state-directed, invested and highly-sophisticated agencies can launch attacks
2 Less Likely	When state-directed individuals or groups can launch attacks
3 Likely	When skilled and organised non-state actors or groups, with or without state sponsorship can launch attacks
4 More Likely	When skilled non-state actors or individuals with commercially available or open software can launch attacks
5 Most Likely	When civilians with basic computer skills can launch such attacks (i.e. internet URLs on web forums for overloading websites)

Table 3: Ordinate Measurement for Likelihood

perpetrated attack – the level of likelihood increases with its score. The five levels of likelihood and their description are presented in *Table 3*.

Thereafter, these data are transferred onto a table which counts the frequency of each threat-likelihood combination. For example, there were 10 incidents with a 'likelihood' score of two and a 'threat' score of one. This table enables the graphing of the bubble chart with the 'threat', 'likelihood' and 'frequency' variables. 'Threat' and 'likelihood' are plotted on the vertical and horizontal axises respectively, while

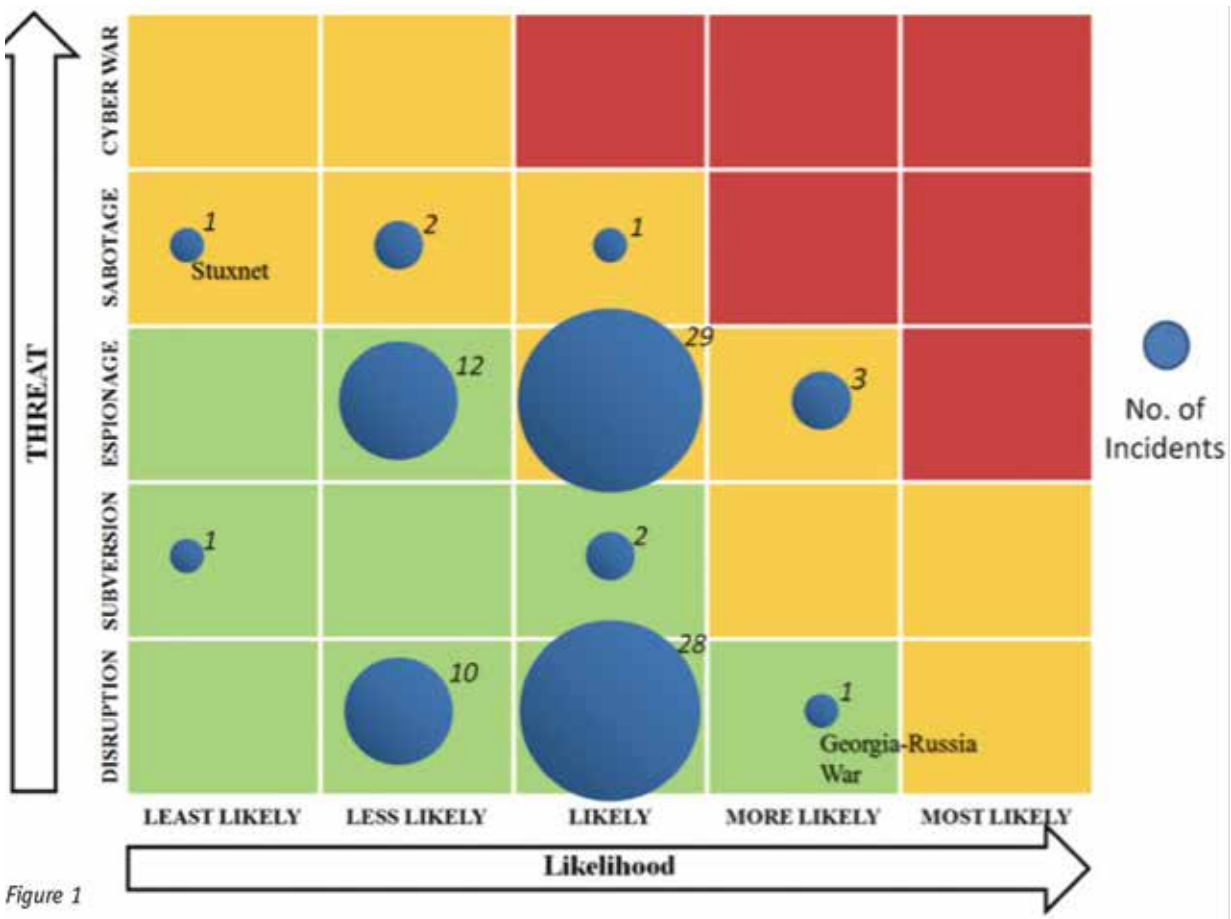


Figure 1

frequency is represented by the size of the bubbles. The bubble chart provides a bird's eye view of the trend of the significant cyber-attacks in recent years and identifies the risk profile of the most prevalent attacks.

Findings

The final chart is set out in *Figure 1* with the frequency listed numerically beside each bubble for convenient reference. By mapping the bubble chart over the risk assessment matrix, several conclusions are clear. Firstly, a majority of the cyber-attacks are low risk incidents, while the rest are in the region of moderate risk. Additionally, there have been no incidents of real cyber war yet. Secondly, skilled and organised non-state or state-sponsored actors mostly conduct espionage and disruption activities which are the most prevalent attacks against states. Thirdly, as attacks become more threatening, they are also less likely to happen as evidenced by the sparse frequency in the top left area of the chart. Finally, and most importantly, current cyber-attacks have not reached the region of high risk where perpetration of attacks is easy and effects are catastrophic at the same time.

Limitations

While these conclusions seem comforting at first sight, there are some limitations to this empirical approach. Firstly, the CSIS list of cyber incidents include only attacks which are deemed 'significant' and is thus, incomprehensive. It provides no clarification on what constitutes significance and there are expectedly numerous other incidents that have been omitted—either because those attacks failed to achieve their objectives or that they were less publicised. Also, states are not inclined to reveal every attack experienced as it may expose their vulnerabilities or impair investigation efforts. Secondly, the difficulty of attributing the perpetrators behind cyber-attacks imposes the difficulty of ascertaining accurately the 'likelihood' scores of the 90 incidents. As a result, several incidents were accorded a 'likelihood' score of three and deemed to be perpetrated by highly-skilled and organised non-state or state-sponsored actors. Nonetheless, this is a reasonable estimate due to the complexity and scale of those attacks. Thirdly, the data measures only incidents and not the number of discrete attacks. Some incidents were composed of several discrete attacks, sometimes amounting to millions of executed attacks such as the hacks against Israeli websites during the 2008-2009 Gaza War. Thus, it is virtually impossible to measure attacks singularly. Furthermore, the various attacks in a specific incident can vary in their threat level, thereby complicating measurement. In such cases, the incident will be accorded a 'threat' score based on its most severe attack. One such incident was the cyber-attacks launched against Georgian government websites during the Georgia-Russia War.[13] In order to circumvent the limitations of the quantitative approach, the next section presents two case studies, each of the most likely and most threatening cyber incidents.

CASE STUDIES: THE GEORGIA-RUSSIA WAR AND STUXNET

This section complements the previous section in assessing the hype of cyber-attacks with analyses from two cases of cyber incidents—the cyber-attacks during the Georgia-Russia War and Stuxnet. These cases were chosen as they each lie on the extreme end of the 'threat' and 'likelihood' spectrum separately. A summary of the significant tenets of these cases will precede an analysis of their lessons.

The Georgia-Russia War

The Georgia-Russia War, against the backdrop of historical geopolitical tensions and other complexities, broke out as a result of Georgia's attack on the Russian-aligned South Ossetian militia. Russia retaliated with an armoured advance, amphibious assault and an intensive artillery bombardment on a Georgian town. In addition, the kinetic assaults were accompanied with a series of cyber operations which in fact, preceded the conventional assaults.[14]

The cyber incidents during the Georgia-Russia War comprised three main types of attacks.[15] The first

was a subversion campaign which defaced Georgian government websites—the most prominent vandalism involved collages of the photographs of Adolf Hitler with the Georgian President for Russian propaganda purposes. The second was a series of distributed denial-of-service attacks that brought down several government, media and corporate websites. The third, and most significant operation involved the setting up of an 'Attack Georgia' website which encouraged the Russian public to download tools as rudimentary as PING utility, which are normally used to test the accessibility of IP addresses, to flood the Georgian cyberspace.[16] A cyber campaign of this scale necessitated preparation, reconnaissance and even war-games. Russian intelligence infiltrated Georgian military and government networks three weeks before the ground campaign to scour for information while cyber militia conducted 'probing attacks' against specified targets in preparation for the actual campaign.[17] Interestingly, Russian cyber militias also attacked a Georgian hacker forum—seemingly as a pre-emptive strike to stem the possibility of a Georgian hackers' retaliation.[18] Furthermore, the cyberspace operations appeared coordinated with Russian conventional ground campaign as hackers attacked local Georgian websites in areas where the military planned on shelling.[19] The Georgia-Russia War is significant as it is a first of its kind where a conventional war was 'integrated' with a cyber-campaign with mass participation.

Engineering such a sophisticated and specific weapon like Stuxnet is no mean feat. Reconnaissance is necessary to map out the target facility's networks and configuration. Intensive technological, programming and engineering prowess are required to design the malware's propagating ability and adaptability.

Stuxnet

The second case study was another game changer as it was the first instance where a cyber-attack resulted in physical destruction.[20] Stuxnet was a highly sophisticated malicious software that was planted in the network of an Iranian nuclear facility in Natanz and designed to gradually deteriorate centrifuges used for uranium enrichment. Natanz functioned on a Microsoft Windows operating system and a Siemens Industrial Control System, but had an 'air gap' which meant that its computers were not connected to the internet.[21] Most likely, Stuxnet had to be inserted into the networks by an unsuspecting staff with an infected thumb drive. Once inserted, Stuxnet was like a living worm. It can propagate and adapt itself in the network; changing its characteristics to avoid detection by antivirus software and firewalls; replicating itself till it identifies the Programmable Logic Controller (PLC) that controls the centrifuges; as well as sending situation reports to its control servers.[22] Stuxnet was to lie dormant until it identifies a PLC connected to a frequency converter that runs the motors of the centrifuges. Thereafter, Stuxnet will begin a sequence to inject a payload designed to disrupt the frequencies of the motors to damage the centrifuges slowly.[23] Meanwhile, the malware is capable of sending deceptive feedback to the human operators to give the impression that the centrifuges were still functioning normally. Nevertheless, the Iranians eventually reached out to open-source security researchers and neutralised Stuxnet. The software vulnerabilities that Stuxnet exploited were quickly patched by Microsoft and Siemens.[24] In the end, Stuxnet only managed to delay Iranian centrifuge programme by a year.[25]

Engineering such a sophisticated and specific weapon like Stuxnet is no mean feat. Reconnaissance is necessary to map out the target facility's networks and configuration. Intensive technological, programming and engineering prowess are required to design the malware's propagating ability and adaptability. Extensive financing is necessary to obtain testing equipment, similar centrifuges and a mock facility for trials and rehearsals. Finally, intelligence networks are

An example of the Siemens Simatic S7-300 PLC CPU that was infected by Stuxnet.

required to plant the malware into the target network. These resources indicate a strong state's involvement. Allegedly, the US National Security Agency and an Israeli intelligence group known as 8200 collaborated to design Stuxnet since the Bush administration.[26] Together, Stuxnet and the cyber incidents in the Georgia-Russia War provide new perspectives on the threat of cyber-attacks against states.

Contesting the Half-Truths of Cyber Attacks

The cyber revolution thesis and political discourse seems to purport that cyber threats can severely threaten nations' security. While there are merits to and advantages of that perspective, it is necessary to balance its half-truths with objective and evidence-based analyses to avoid spiralling threat conflation. The research in this essay suggests that as yet, the threat of cyber-attacks to states is overrated.

One of the tenets of the cyber revolution thesis asserts that cyber-attacks can take place independently of traditional military systems. While this is possible, my findings suggest that attacks that take place solely in the cyber domain may only marginally compromise a state's monopoly of legitimate force at best, but are unable to infringe upon a state's territorial integrity. The case of the Russia-Georgia War demonstrates the importance of 'boots-on-the-ground' to overpower the opponents' militaries and occupy territories. While the accompanying cyber campaign was impressive, they were nothing but cyber vandalism and a nuisance. Stuxnet demonstrates the case of a standalone cyber-attack which damaged physical infrastructure—a case of an arguably significant threat to a state. Yet, for a highly invested and sophisticated cyber weapon to only achieve a limited effect of destroying 11.5% of the 8,500 Iranian centrifuges, barely above the centrifuges' typical breakdown rate, this more than adequately proved that cyber-attacks independent of traditional military systems can only marginally compromise a state's monopoly of violence.[27]

Perhaps the most accepted claim of the cyber revolution thesis is the difficulty of attribution and the anonymity of cyber-attacks. While I concur with the claim, attribution is not entirely impossible. In fact, most cyber-attacks remain anonymous because they are 'an inconsequential nuisance' that do not warrant a full-scale investigation.[28] On the other hand, most incidents with a 'threat' score of four on the bubble chart can be attributed. The circumstantial evidence of Stuxnet for example, inadvertently points to possible US and Israeli collaboration. Additionally, anonymity can be a burden for its perpetrators. Actors intending to initiate cyber-attacks must undertake considerable measures to maintain anonymity. As the complexity and intended threat of an attack increases, the risk of attribution increases consequently as states are also more likely to investigate incidents of greater significance.

Another claim advances the asymmetric nature of cyber-attacks and its low entry barriers which facilitate its exploitation by non-state actors or weak states. As the Stuxnet case study demonstrates, cyber-attacks on the higher end of the 'threat' spectrum are contrary to the asymmetric claim. Effective cyber weapons are costly and impose high technology barriers beyond the reach of non-state actors such as terrorist groups. Furthermore, they often do not guarantee success and are surgical and 'one-shot' in nature. Hence, it is more rational for non-state actors to resort to conventional tactics with higher rates of success at much lower costs.

Cyber-attacks are also cited as inherent with a zero-sum paradox where technologically advanced states are empowered and vulnerable at the same time. The findings in this essay however, demonstrate that the paradox is exaggerated. As the bubble chart shows, disruption and espionage are the most prevalent cyber-attacks to plague the most technologically advanced states; but they do not threaten the state's territorial integrity and monopoly of legitimate force. Furthermore, vulnerability in cyberspace is less severe than in the physical domain. Stuxnet shows that disruption or damages as a result of cyber-attacks can be quickly recovered or replaced, unlike the irreversible destruction that kinetic force inflicts.

In the long run, cyber offence cannot keep up with defence as defenders learn the modus operandi of cyber-attacks.

Cyber revolution theorists also highlight that cyberspace is primarily offence-dominant but my findings suggest that defence will be increasingly easier. Firstly, while cyber disruption and espionage are relatively easier to conduct, cyber operations with physical offensive implications such as sabotages are still few and costly. Yet, while strong states can reasonably afford to produce costly and complex cyber weapons for offensive purposes, the costs of defence and recovery for the defending state is significantly lower.[29] Stuxnet for example, had enthusiastic technological corporations rushing to patch and neutralise on behalf of their Iranian clients. Additionally, the codes of several malicious cyber weapons, including Conficker and Stuxnet, are presently available on the internet along with instructions for repair and recovery. In the long run, cyber offence cannot keep up with defence as defenders learn the modus operandi of cyber-attacks.[30]

Most alarmingly, the academic and political discourse is interspersed with claims that cyber threat is catastrophic. As yet, the bubble chart shows that current cyber incidents have not reached the region of high risk and are unable to inflict widespread infrastructural damages and civilian casualties. If Stuxnet can be benchmarked as the most threatening cyber weapon currently, it would take astronomical investments and massive collaboration to wage an entire cyber war capable of deposing a sovereign state's monopoly of force. Intuitively however, conventional military forces are still necessary to breach its territorial integrity and occupy territories. Of course, this is a purely deductive conjecture as cyber-attacks may still be in their infancy.

DEFENCE AS A TENABLE CYBER STRATEGY?

The findings in this essay provide some principles for a tenable cyber strategy. The bubble chart and risk assessment reveal disruption and espionage activities as the most prevalent attacks. While the case studies suggest that disruption activities are merely cyber nuisance, espionage is an already prevalent phenomenon that is merely facilitated by the cyber domain but definitely falls short of revolutionary. Additionally, recovery and defence is faster and more cost-effective than offensive tactics in the absence of catastrophic cyber war which, as evidenced by Stuxnet, would require astronomical cost and effort with no guarantee of success. Without conventional military force, cyber-attacks are unable to effectively diminish a state's monopoly of force or compromise its territorial integrity. Therefore, a tenable cyber strategy in the near term should primarily be defence-oriented. Firstly, the establishment of rapid recovery capabilities can minimise the impact of disruption and subversion activities, while attribution capabilities can potentially deter aggressors. Next, deceptive counter-intelligence and management discipline of human operators—the weakest link in the entire cyber infrastructure—can mitigate cyber espionage. Last but not least, reconnaissance and other intelligence activities are useful for early warnings as both Stuxnet and the Georgia-Russia War demonstrated that rehearsals do take place before major cyber-attacks.

CONCLUSION

This essay has demonstrated that the hype asserting that cyber-attacks threaten the security of states is

overrated. The empirical study of recent cyber-attacks show that the risk profile of these attacks are in the region of low to moderate risk—mostly disruption and espionage activities—and that no incidents of cyber war has occurred. The case studies countered the claims of the cyber revolution thesis and showed that they mostly portray half-truths. While the cyber domain indeed presents new challenges and difficulties for the security of states, in reality cyber-attacks do not yet possess the capacity to effectively depose a state's monopoly of force or infringe on its territorial integrity. Feeding the hype and frenzy of catastrophic cyber-attacks will engender unnecessary fears and perceived vulnerabilities, leading to greater militarisation of cyberspace and ironically, increased and perhaps irrational insecurity. In this vein, a defensive cyber strategy focused on recovery and attribution capabilities, counter-intelligence and personnel discipline and reconnaissance is rational and tenable in the short term.

BIBLIOGRAPHY

Adams, J. "Virtual Defence." *Foreign Affairs,* 80(3), (2001).

Albright, D., Brannan, P., and Walrond, A. C. "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security* (2010).

Baldwin, D. A. The Concept of Security. Review of International Studies, (1997), 5-26.

Buzan B., Wæver, Ole, and Wilde, Jaap De. Security: A New Framework for Analysis (Boulder: Lynne Rienner Publishers, 1998).

Cox, L.A. "What's Wrong with Risk Matrices." *Risk Analysis* 28, n._2 (2008), 497-512. Data Exchange Agency. "Cyber Attacks Against Georgia." *Ministry of Justice of Georgia,* 2011.

Haddick R. "This Week at War; Lessons from Cyber War 1." *Foreign Policy,* 2011. http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i.

Hollis, D. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal,* (2011).

Keizer, G. "Russian Hacker 'Militia' Mobilises to Attack Georgia." Computer World, accessed November, 2013. http://www.computerworld.com/s/article/9112443/Russian_hacker_militia_to_attack_Georgia

Krepenevich, A. F. Cyber Warfare: A "Nuclear Option"? *Centre for Strategic and Budgetary Assessments,* 2002.

Lindsay, J. R. "Stuxnet and the Limits of Cyber Warfare," *Security Studies,* (2013).

MITRE. *Risk Management Tools.* http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools

Panetta, L. "CIA Chief Leon Panetta: Cyber Attack Could is 'Next Pearl Harbour'." *Huffington Post,* June, 2011. http://www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html.

Pierson, C. The Modern State (London: Routledge), 1996.

Rid, T. "Cyber War Will Not Take Place." *The Journal of Strategic Studies* 35, n._1, (2012), 5-32.

Sanger, D. E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown), 2012.

Schreier, F. "On Cyberwarfare." *DCAF Horizon 2015 Working Paper No. 7,* n.d.

Shimeall, T., Williams, P., and Dunlevy, C. "Countering Cyber War." *NATO Review 49,* n._4, (2001): 16-18.

Tabansky, L. "Basic Concepts in Cyber Warfare." *Military and Strategic Affairs* 3, n._1 (2011): 75-92.

Tilly, C. The Formation of National States in Western Europe (Princeton: Princeton University Press), 1975.

L. Valeri, and M. Knights. "Affecting Trust: Terrorism, Internet and Offensive Information Warfare." *Terrorism and Political Violence* 12, n._1 (2000), 15-36.

Wall Street Journal. "Cyber Combat: Act of War," May 21, 2011. http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718.

Weber, M. "Politics as a Vocation". in H. H. Garth, and C.W. Mills. *Essays in Sociology*. (New York: Macmillian, 1946), 26-45.

Wolfers, A. "'National Security' as an Ambiguous Symbol." *Political Science Quarterly* 67, n._4 (1952), 481-582.

ENDNOTES

1. Panetta, Leon. *Cyber Attack Could be 'Next Pearl Harbour'*. Huffington Post, June 2011. http://www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html.
2. Barry Buzan, Ole Wæver, and Jaap De Wilde, *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

3. Wall Street Journal, *Cyber Combat: Act of War,* May 2011. http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718.

4. L. Tabansky, *Basic Concepts in Cyber Warfare,* Military and Strategic Affairs 3, n._1, 2011; F. Schreier, *On Cyberwarfare,* DCAF Horizon 2015 Working Paper No. 7, n.d.

5. Schreier, *On Cyberwarfare;* A. F. Krepenevich, *Cyber Warfare: A "Nuclear Option"?* Centre for Strategic and Budgetary Assessments, 2002.

6. M. Weber, *Politics as a Vocation,* in H. H. Garth, and C.W. Mills, *Essays in Sociology,* (New York: Macmillian), 26-45;

7. C. Pierson, *The Modern State,* (London: Routledge, 1996).

8. B. Buzan, *People, States and Fear: The National Security Problem in International Relations,* (North Carolina: University of North Carolina Press, 1983).

9. D. A. Baldwin, "The Concept of Security", *Review of International Studies* (1997), 13.

10. Centre for Strategic and International Studies, *Significant Cyber Incidents Since 2006,* accessed November, 2013. The list is a work in progress subjected to regular updates by the CSIS and the data used in this essay is correct as of the accessed date.

11. L. A. Cox, "What's Wrong with Risk Matrices," *Risk Analyses* 28, n._2 (2008). While risk assessment matrices vary according to organisations and contexts, the threat and likelihood matrix is a widely used tool in organisations such as the American Federal Aviation Administration among other applications such as for terrorism risk analyses, climate change risk management and military safety and risk management.

12. MITRE, *Risk Management Tools* http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools.

13. T. Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, n._ 1 (2012), 13.

14. D. Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal* (2011).

15. T Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, n._ 1 (2012).

16. Data Exchange Agency, *Cyber Attacks Against Georgia,* Ministry of Justice of Georgia, 2011, 11.

17. R. Haddick, "This Week at War; Lessons from Cyber War 1,"Foreign Policy, 2011, http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i; Hollis, "Cyberwar Case Study".

18. G. Keizer, *Russian Hacker 'Militia' Mobilises to Attack Georgia,* Computer World, November, 2013. http://www.computerworld.com/s/article/9112443/Russian_hacker_militia_mobilizes_to_attack_Georgia.

19. D. Hollis, "Cyberwar Case Study: Georgia 2008." *Small Wars Journal,* (2011).

20. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* (2013).

21. T. Rid, *Cyber War Will Not Take Place,* The Journal of Strategic Studies 35, n._ 1 (2012), 18.

22. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* (2013), 382.

23. Ibid., 384.

24. Ibid., 394.

25. Ibid., 390.

26. D. E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,* New York: Crown, 2012.

27. D. Albright, P. Brannan, and A. C. Walrond, *Did Stuxnet Take out 1000 Centrifuges at the Natanz Enrichment Plant?,* Institute for Science and International Security, 2010.

28. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* (2013), 401.

29. Ibid.

30. T. Shimeall, P. Williams, and C. Dunlevy,"Countering Cyber War", *NATO Review* 49, No. 4, 2001.

CPT Lim Ming Liang is an Armour Infantry Officer by vocation and is currently a Staff Officer in HQ Armour. He received the SAF Academic Scholarship and graduated from the National University of Singapore with a Bachelors of Social Sciences (Honours) in Political Science.

Contested Territory: Social Media and the Battle for Hearts and Minds

by **CPT Lau Jian Sheng, Jason**

Abstract:

Throughout history, military forces around the world have faced a similar challenge—garnering civilian support for their activities. Militaries are cognisant that their potency rests not only on their offensive capability, but also on the resolute backing of the entire population. Consequently, militaries are compelled to actively secure the wider public's commitment to defence. This is a vital task even for the world's most powerful military, the United States. Singapore is no exception. It is likely that the formulation of Total Defence as a security philosophy for Singapore was inspired by earlier models such as Switzerland's 'General Defence' and Austria's 'Comprehensive National Defence'. Psychological defence is one of the five pillars of Total Defence. The foundation for this robust pillar of psychological defence has been continual engagement with the populace and the media's impact on fostering commitment to defence is most critical. Singapore's defence strategy that e ncompasses c ultivating a national consensus has come under mounting pressure in recent years, with media consumption patterns shifting from the mainstream mass media to online social media. The author concludes that in the long run, it is timely to open up to public dialogue and deeper personal engagement, as in the contest for hearts and minds, a tight-fisted regulation of social media may yet win the battle but lose the war.

Keywords: National Consensus, Social Media, Commitment to Defence, Continual Engagement

INTRODUCTION

The age-old challenge for militaries—engaging the people and instilling the will to fight

Military forces around the world have faced a similar challenge throughout history—garnering civilian support for their activities. Militaries are cognisant that their potency rests not only on their offensive capability, but also on the resolute backing of the entire population. Sun Tzu, the classical military theorist, observed that "[he] whose ranks are united in purpose will be victorious."[1] A united community provides for a legitimacy of purpose and lends emotional support and genuine physical assistance for troops. Therein lies the importance of engagement.

Consequently, militaries are compelled to actively secure the wider public's commitment to defence. This is a vital task even for the world's most powerful military. Admiral Mike Mullen, then the Chairman of the Joint Chiefs of Staff, stated at a conference in 2011 that the United States military "[could not] afford to be out of touch with [the people...] we cannot survive without their support—across the board."[2]

Singapore's approach to engagement

Singapore is no exception. Engagement was the impetus for the introduction of the Total Defence construct in 1984. Mr. Goh Chok Tong, then Minister for Defence, announced unequivocally that the "SAF wants to strengthen its ties with you."[3] In fact, his speech simultaneously marked the launch of the SAF Story exhibition at various community centres nationwide. This was aimed precisely at deepening engagement with the Singaporean public.

The formulation of Total Defence as a security philosophy for Singapore was likely to have been

inspired by earlier models such as Switzerland's 'General Defense' (1973)[4] and Austria's 'Comprehensive National Defense' (1975).[5] 'Total Defence' advanced two main ideas: (i) defence as everyone's responsibility—involving all; and (ii) defence as an ongoing, perpetual concern, from peacetime to war. It rested on five pillars: psychological defence, civil defence, social defence, economic defence and military defence (see *Figure 1*). These pillars were concerned with ensuring a collective will to defend the country, protection of civil resources, cohesion between diverse sub-communities, economic growth to sustain defence spending and military might itself.[6]

The pillar of psychological defence is the primary focus of this essay. Psychological defence means that "Singaporeans [who] are united in pride and passion for our country... will stand up to defend what is ours and protect our independence as a nation... whatever the crisis or challenge."[7] This resilience has seen the country through trials as significant as the SARS crisis of 2003 and the Jemaah Islamiyah terrorist threat from the mid-1990s.[9]

Yet the foundation for this robust pillar of psychological defence has been continual engagement with the populace. Total Defence activities are a means of reaching out to the Singaporean public, and the Singaporean public having thus been engaged, in turn contribute to Total Defence. Over the years, national unity and commitment to defence have been cultivated through institutions and programmes such as the annual Total Defence Award which recognises employers who demonstrate strong commitment to defence; the SAF-Schools Partnership Programme, which exposes students to defence matters; and the Advisory Council for Community Relations in Defence (ACCORD), which is a body of grassroots leaders and community stakeholders who provide feedback to the Minister for Defence.[10]

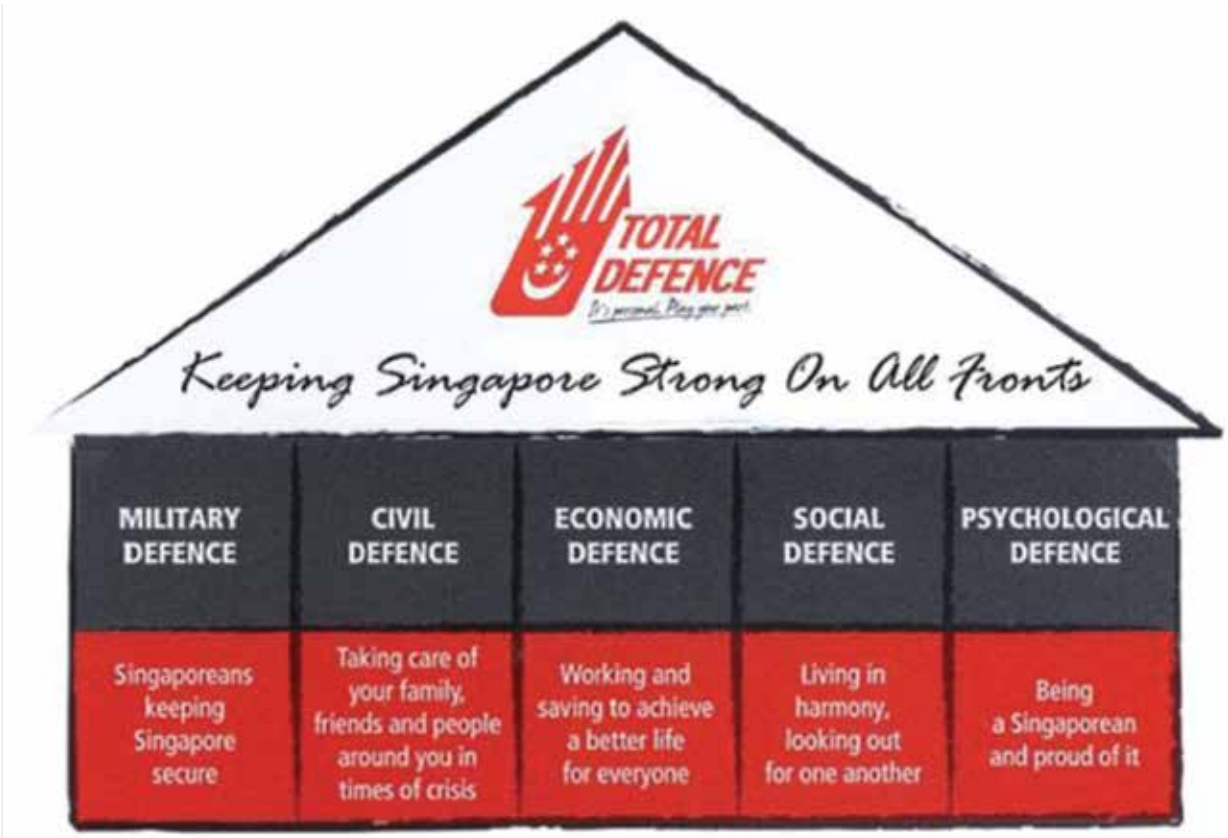


Figure 1: The Five Pillars of Total Defence[8]

The restructured Advisory Council on Community Relations in Defence (ACCORD)(Main) held its first meeting at SAFRA Toa Payoh on 25th August 2014, chaired by Second Minister for Defence, Mr Chan Chun Sing and supported by Deputy Chairman, Minister of State for Defence, Dr Mohamad Maliki Bin Osman.

THE MEDIA'S PIVOTAL ROLE IN ENGAGING THE PUBLIC

However, it is the media's impact on fostering commitment to defence that is arguably second to none. The mass media's pervading presence is evident in everyday material like television advertisements aimed at recruitment and newspaper reports of successful humanitarian missions. The persistent positive messaging contributes significantly to the collective's pro-defence orientation.

The media's pivotal role in public engagement should be understood in the following manner. Because of our finite capacity for first-hand experience, the media are "our window onto the world, and onto ourselves."[11] They condition our understanding of reality and "shape the process of thought."[12] When the media communicate events, ideas and aspects of culture, they simultaneously influence and persuade. The expansive outreach of the mass media enables them to shape public opinion by setting the news agenda,[13] framing events in particular ways,[14] and priming audience responses.[15] In essence, the media steer public consciousness. Manuel Castells, the influential communications theorist, even goes so far as to assert that "what does not exist in the media does not exist in the public mind, even if it could have a fragmented presence in individual minds."[16]

Consequently, the mass media, which has been the predominant system of communication in the modern era, serves an essential function. They operate under the auspices of political actors to forge consensus within society and, in the case of the military, to foster commitment to defence. This system of communication produces 'a relatively controlled public sphere'[17] as "the ideology of the elite is [constantly] reaffirmed, and counter-ideologies are suppressed."[18]

In Singapore, the government and the mass media have historically been a tightly-knit pair. The government either owns or otherwise indirectly influences the endeavours of the two dominant mass media corporations in Singapore: Mediacorp[19] and Singapore Press Holdings.[20] The Parliament has also passed a set of legislative rules that clearly defines what the media can and cannot do. These include Article 14 of the Singapore Constitution,[21] and various acts of Parliament such as the Newspaper and Printing Presses Act (2002),[22] and the Broadcasting Act (2012).[23]

This close supervision of the mass media is largely due to a political conviction that the survival and success of Singapore is contingent on consensus and a united front. Then-Prime Minister Lee Kuan Yew was adamant that the media could not follow the liberal Western model of the Fourth Estate and, instead had to be "subordinated to the definition and integrity of the nation."[24] This conviction was forged in the crucible of racial and religious cleavages and remains unchanged today. In fact, the same beliefs were more recently echoed by the Minister for Communications and Information, Dr. Yaacob Ibrahim. He professed that Singapore's media model is "based on forging consensus and facilitating nation-building... [on] information and viewpoints that inform and evaluate, and not disturb and divide."[25]

Because of our finite capacity for first-hand experience, the media are "our window onto the world, and onto ourselves."

THE DISRUPTIVE IMPACT OF SOCIAL MEDIA

Given the mass media's well-defined role in public engagement and social media, it presents a new media environment that constitutes a

In conjunction with the Ministry of Defence's 2012 NS45 campaign, Jack Neo's film Ah Boys to Men sets to commemorate the 45th anniversary of Singapore's National Service and foster commitment to defence.

contemporary information revolution with their unique characteristics.[26]

Defining social media

Juxtaposed against the mass media, social media is a comparatively recent phenomenon. It is a subset of Internet media, but there are crucial differences. Social media belong to the realm of Web 2.0 and are characterised by connectivity, interactivity and individual expression.[27] While earlier developments such as e-mail and websites may have paved the way for online interaction, social media offers a qualitatively different experience. The ethos of social media is participation and collaboration.[28] Social media users belong to an active community, otherwise known as the 'networked public'.[30] Examples of social media include social networking sites such as Facebook, Google+ and LinkedIn; blogs, vlogs and streamable or downloadable podcasts; community-based websites such as Wikipedia; online forums; and social networking tools such as Twitter, Tumblr, YouTube, Flickr, Reddit, Digg, del.icio.us and RSS. Ultimately, social media, as their name suggests, is about 'making connections'.[31]

High rates of social media usage in Singapore

From about the turn of the century, social media has been burgeoning in popularity. Today, Singapore is 'one of the most evolved social media markets'.[32] She is ranked 16th out of 138 countries on an index that measured the use of virtual social networks in 2011.[33]

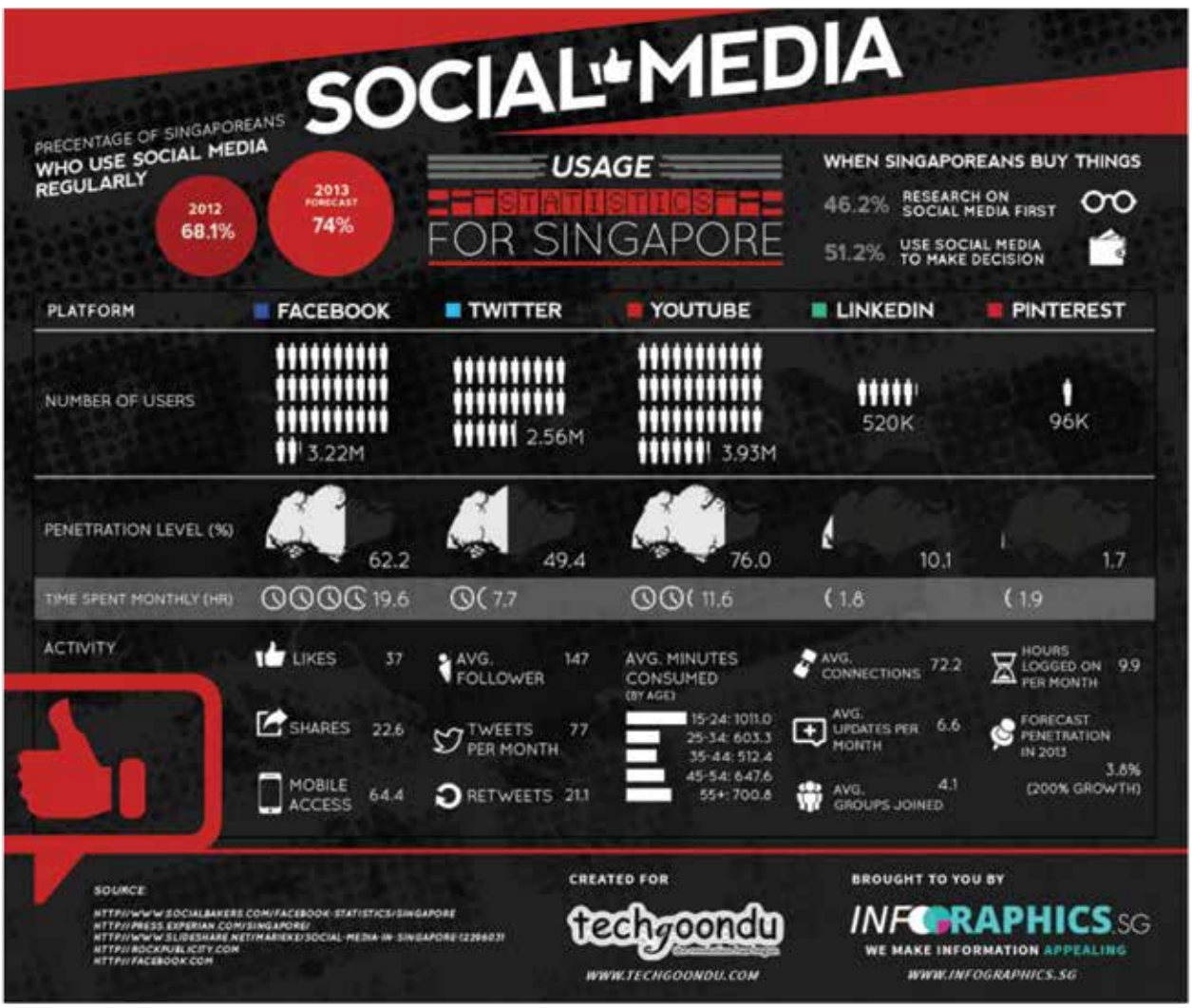


Figure 2: Infographic depicting social media usage in Singapore in 2012 [29]

In 2012, 76% of the 5.2 million strong population watched YouTube videos, while another 62% frequented Facebook and 49% accessed Twitter regularly (see Figure 2).[34] 61% of the digital users in Singapore also visit online forums monthly.[35] Collectively, these users spend twice as much time accessing online media as compared to watching television, or five times as much time as compared to reading newspapers.[36]

This reflects a pertinent shift in media consumption patterns, away from the mainstream mass media and towards online social media.[37] One of the catalysts in supporting this trend is mobile access to internet technologies. Singapore has the highest smartphone penetration per capita in the world and Internet-enabled smartphones facilitate perpetual and ubiquitous connectivity to social media. According to Nichola Rastrick, the managing director of Millward Brown in Singapore, social media "[has] become a functional part of the new Singaporean lifestyle [serving as the platform] where Singaporeans gather news, discuss social issues, arrange social gatherings... create professional networks [...] and decide what to eat, buy and collect."[38]

Social media effects and implications

With the advent of social media, the mass media no longer retain their monopoly over public consciousness. The public sphere is relatively less controlled, as individuals are empowered on two counts: firstly, to speak up and be heard and secondly, to form their own conclusions on the basis of first-hand access to information. This individual empowerment means that social media are often purveyors of alternative, more-personalised accounts, while the mass media typically remain as outlets for mainstream or establishment views. Although it is over-simplistic to conflate them so readily into opposing camps, there is a genuine sense of communicative or journalistic autonomy on social media.[39] This also leads to an unprecedented diversity of information, which individuals can access to broaden their perspectives.

Faced with the plethora of opinions, defence policies will be critically scrutinised like never before, and policymakers will be driven to answer difficult questions that may not have previously arisen.[40] For instance, blog posts such as those by David Boey, criticising the defence establishment for a lack of transparency in accounting for deaths in the SAF, or Gordon Lee, proposing to dispose of National Service (NS) in favour of a larger regular force backed up by a volunteer reserve force, will be increasingly common.[41] This unfettered contest of ideas will inevitably lead to a weakened unity of mindset and the possible dissolution of a fragile national consensus—the implication seemingly being that citizens in this newly-fragmented society will be less willing to face up to national challenges together.

This individual empowerment means that social media are often purveyors of alternative, more-personalised accounts, while the mass media typically remain as outlets for mainstream or establishment views.

Yet this dystopia may be more imaginary than realistic. While there is a relative lack of publicly available longitudinal data for meaningful analysis, the data at hand does not support the thesis that national commitment to defence has been compromised. Surveys conducted in 1993 and 1999 by the Institute of Policy Studies (IPS) found that survey respondents in the later survey were more likely to agree with the statement that "Singapore is worth defending no matter what is the cost to me" and conversely disagree with the statement that "In the event of war, I will leave Singapore."[42] Even more recently, the independent study commissioned by the Committee to Strengthen National Service in 2013 found that more than 98% of survey respondents agreed with the statements that "NS is necessary for the defence of Singapore" and "NS provides the security needed for Singapore to develop and prosper."[43] These statistics, when taken at face value, indicate that the impact of social media on national unity and commitment to defence is not as damaging as previously imagined.

In actuality, the use of social media can reap positive benefits for the nation-state. The ease of publication on this medium allows individuals to articulate useful critiques and constructive suggestions. On the other hand, the online community can be self-policing, with disparaging and unhelpful posts censured and discouraged by commenting peers. This was evident in the case of the STOMPer who was rebuked by netizens for criticising an NSman for drinking water on the train (Figure 3). Given that these responses were coming from members of the same virtual community, they were considered more authentic than official replies and their voices consequently carried more weight.

As citizens are empowered to participate in online discussions, they will be engaged at a deeper cognitive level than before. Instead of being on the receiving end of information, they can be actively involved in the co-creation of new information. With social media, it is perhaps the case that engagement is enhanced, rather than being undermined.

JUMPING ON THE BANDWAGON: THE SAF'S FORAY INTO SOCIAL MEDIA

To cater to the changing media consumption patterns, the SAF has tentatively ventured into the field of social media. In 2007, MINDEF introduced N.E.mation!, a digital animation contest for students. This annual competition centres on various Total Defence themes, with viewers voting online to determine the eventual winners.[45] In the more conventional social media space, MINDEF has also established an online presence. Cyberpioneer, the online complement of the Pioneer magazine, is now available on YouTube, Facebook, Flickr and Twitter.[46]

Within one year from its launch in 2008, views on the Cyberpioneer YouTube channel increased tenfold from 200,000 to 2 million. Popular CyberpioneerTV video series include *Every Singaporean Son* and special features on elite units such as the Commandos or the Naval Diving Unit. Individual services have also got involved with social media. In 2011, the RSN created a website entitled the *'Sea of Support'*, which allowed family and friends to post messages of goodwill and support to navy personnel who had sailed off to serve in the Gulf of Aden.[47]

To regulate the use of social media at the level of the individual, MINDEF and the SAF created a Code of Conduct on Social Media Participation.[48] This Code of Conduct is targeted at in-service personnel and

Figure 3: Post on STOMP criticising an NS personnel and sampled comments.[44]

provides a useful list of 'dos and don'ts' on social media. The guiding principles are summarised accordingly:[49]

1. Be Responsible: be yourself, observe operational security and own what you say.

2. Be Professional: uphold the highest standards of leadership, personal conduct and professionalism, both offline and online.

3. Be Reliable: speak the truth and know what you are saying.

4. Be Respectful: be respectful during online conversations and sensitive to the type of comments you make.

5. Be Receptive: practise deep listening and quality conversations.

6. Be Safe: adjust your social media privacy and security settings to prevent personal data from being compromised.

7. Be Ethical: behave and converse online as you would in a public face-to-face conversation.

This form of genuine engagement will encourage well-meaning social media contributors to provide a constant supply of reasoned, alternative arguments and will further strengthen commitment to defence by making them active stakeholders in policy decisions.

Do note that as it is on social media that individuals gain the liberty to express themselves freely, it is almost naive to assume that this freedom would be so easily and willingly surrendered or curtailed. It is not that the guidelines are not relevant; they are well-intentioned but impossible to administrate. There is no realistic means of enforcing social media regulations, short of archaic throwbacks to hardline censorship via Internet Service Provider (ISP) blocking or gazetting of websites. Restricting, or being viewed as attempting to restrict, social media activities may ultimately lead to greater discontent and disengagement. The traditional form of top-down control is incompatible with the technical architecture of the medium, which is about lateral connections. Social media, as a democratising phenomenon, need to be more clearly understood to be better utilised.

PROPOSITIONS AND RECOMMENDATIONS

In the age of social media, the new reality is a plurality of media accounts. Instead of trying to control the conversations on social media, we need to accept and be accustomed to the diversity and variety of opinions. This is perhaps the most significant mindset shift required.

The well-regulated information regime is a thing of the past. The emphasis, henceforth, should shift towards developing new media literacies and critical thinking skills, as well as educating discerning citizens to sift through the subjective 'noise'. An educated, politically aware and technologically empowered citizenry will have the wherewithal and the gumption to critique policies that have long been accepted as sound and immutable. This may be viewed as an advancement of public dialogue and an opportunity to relook policies and their assumptions, rather than as an interminable slide towards populism.

As conversations are allowed to flourish, the diversity of opinions can be leveraged to widen policy considerations and uncover hitherto hidden grievances and other blind spots. New ideas such as the conscription of females and the imposition of a National Defence tax on foreigners can be thoroughly debated even before entering the courts of lawmakers.[50] The desired end-state amidst this flurry of ideas are people who speak up.

As in-service personnel, we should respect the social media ethos and engage as individuals, person-to-person, and not behind a wall of bureaucracy. We should be authentic, sharing "what we believe in [and] not blindly [trumpeting] positive messages."[51]

While engaging on social media, we should follow up with relevant actions in the real world, since that is the object of engagement. This form of genuine engagement will encourage well-meaning social media contributors to provide a constant supply of reasoned, alternative arguments and will further strengthen commitment to defence by making them active stakeholders in policy decisions.

CONCLUSION

Singapore's defence strategy has encompassed cultivating a national consensus that is strong enough to overcome racial, religious and other communal differences. This consensus has come under mounting pressure in recent years, with media consumption patterns shifting from the mainstream mass media to online social media. Yet the jury is out on the impact of social media. What is undisputed is that they have a unique set of characteristics and that there is a new medium of communication. The new reality of information heterogeneity must be embraced and the ethos of participation and collaboration clearly grasped. It is time to open up to public dialogue and deeper personal engagement, as in the contest for hearts and minds, a tight-fisted regulation of social media may yet win the battle but lose the war

BIBLIOGRAPHY

Ahonen, T. Smartphone Penetration Rates by Country! We Have Good Data (finally), 12 December 2011. *Communities Dominate Brands,* available online: http://communities-dominate.blogs.com/brands/2011/12/smartphone-penetration-rates-by-country-we-have-good-data-finally.html (accessed 20 November 2013).

Benkler, Y. *The Wealth of Networks: How Social Production Transforms Markets and Freedom,* (New Haven: Yale University Press, 2006).

Bimber, B. 'How Information Shapes Political Institutions' in D.A. Graber (Ed.) *Media Power in Politics,* (Washington: CQ Press, 2011), 5-17.

Boey, D. Coming to terms with Singapore Armed Forces (SAF) Training Deaths, 6 April 2012. *Senang Diri,* available online: http://kementah.blogspot.sg/2012/04/coming-to-terms-with-singapore-armed.html

Bokhorst-Heng, W. Newspapers in Singapore: a mass ceremony in the imagining of the nation. *Media, Culture & Society,* 24, n._4 (2002), 559-569.

Broadcasting Act (2012), Chapter 28, Singapore, available online: statutes.agc.gov.sg/

Carr, N. Is Google Making us Stupid? *Yearbook of the National Society for the Study of Education,* 107, n._2 (2008), 89-94. Carr, N. *The Shallows: What the Internet is Doing to Our Brains,* (New York: W.W. Norton & Company, 2010).

Castells, M. Communication, Power and Counter-power in the Network Society. *International Journal of Communication,* 1, n._1 (2007), 238-266.

Chua, T. Singapore is one of the world's most evolved social media markets, 10 February 2011. *Singapore Business Review:* available online: http://sbr.com.sg/media-marketing/news/singapore-one-world%E2%80%99s-most-evolved-social-media-markets

Domke, D., Shah, D.V. and Wackman, D.B. Media Priming Effects: Accessibility, Association, and Activation. *International Journal of Public Opinion Research,* 10, n._1 (1998), 51-74.

Dutta, S. and Mia, I. *The Global Information Technology Report 2010-2011: Transformations 2.0,* (Geneva: World Economic Forum, 2011).

Fenton, N. 'Drowning or Waving? New Media, Journalism and Democracy' in N. Fenton (Ed.) *New Media, Old News,* (London: SAGE, 2010), 3-16.

Frank, J. 'A Neutral's Perspective: The Role of the Austrian Armed Forces in Homeland Security' in J.L. Clark (Ed.) *Armies in Homeland Security: American and European Perspectives,* (Washington DC: National Defence University Press, 2006), 119-148.

George, C. Freedom From The Press: Why The Media Are The Way They Are, 25 October 2001. *Air-Conditioned Nation,* available online: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN004067.pdf

Goh, C.T. Speech by Mr Goh Chok Tong, Minister of Defence and Second Minister for Health, at the Official Opening of "The SAF Story Exhibition", *Singapore Government Press Release,* 5 January 1984.

Gomez, J. Restricting Free Speech: The Impact on Opposition Parties in Singapore. *The Copenhagen Journal of Asian Studies,* 23, n._1 (2006), 105-131.

Griffith, S.B. *Sun Tzu: The Art of War,* (London: Watkins Publishing, 2011).

Hopmingu NS guy should have known better than to drink on train, 22 November 2013. *STOMP,* available online: http://singaporeseen.stomp.com.sg/singaporeseen/hey-goondus/ns-guy-should-have-known-better-than-to-drink-on-train-while-in-uniform

Ibrahim, Y. Traditional and online media is the new normal [speech], Singapore Press Club Lunch, 23 April 2012. *MICA Press Releases and Speeches,* available online: http://app.mica.gov.sg/Default.aspx?tabid=79&ctl=Details&mid=540&ItemID=1393

Infographics.SG *Social Media Usage Statistics for Singapore,* 7 June 2013, available online: http://infographics.sg/?portfolio=social-media-usage-statistics-for-singapore-static-infographic

Institute of Policy Studies (2000) *Citizens and the Nation - IPS Survey of National Pride and Citizens' Psychological Ties to the Nation* [press release], Singapore: Institute of Policy Studies, available online: http://lkyspp.nus.edu.sg/ips/wp-content/uploads/sites/2/2013/06/Press-Citizens-and-the-Nation-web.pdf

Kaplan, A.M. and Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons,* 53, n._1 (2010), 59-68.

Lasswell, H.D. (2007) The structure and function of communication in society. *Journal of Communication Theory and Research,* 24 (Winter-Spring), 215-228.

Lee, G. National Service - by Guest Spot Author Gordon Lee, 8 April 2011. *Rethinking the Rice Bowl: Tackling the Economic Questions as Singapore Transitions from Authoritarianism to Democracy,* available online: http://sonofadud.com/2011/04/08/ns/

Leong, C-H., Yang, W.W. and Ho, M.W.H. (2013) *Singaporeans' Attitudes to National Service* [presentation slides], Singapore: Institute of Policy Studies, available online: http://lkyspp.nus.edu.sg/ips/wp-content/uploads/sites/2/2013/04/NS-study-8-Oct-2013_web.pdf

Li, C. and Bernoff, J. *Groundswell: winning in a world transformed by social technologies* [e-book], (Boston: Harvard Business Review Press, 2011).

Lim, S.S. and Nekmat, E. '*Media Education in Singapore* – New Media, New Literacies?' in C. Cheung (Ed.) Media Education in Asia, (Dordrecht: Springer, 2009), 185-197.

Matthews, R. and Yan, N.Z. Small Country 'Total Defence': A Case Study of Singapore. *Defence Studies,* 7, n._3 (2007), 376-395.

McCombs, M.E. and Shaw, D.L. The Agenda-Setting Function of Mass Media. *Public Opinion Quarterly,* 36, n._2 (1972), 176-187.

Ministry of Defence Public Affairs, *MINDEF/SAF Code of Conduct on Social Media Participation,* March 2013.

Ministry of Education *Total Defence Day 2013,* 15 February 2013, available online: http://www.ne.edu.sg/files/Total%20Defence%20Day%202013.pdf

Ministry of Home Affairs *The Jemaah Islamiyah Arrests and the Threat of Terrorism* [White Paper], Cmd. 2 of 2003, (Singapore: MHA, 2003).

Mullen, M. JCS Speech. *NDU Conference on Military Professionalism,* 10 January 2011, Washington DC: National Defense University, available online: http://www.jcs.mil/speech.aspx?id=1517

Muthhukumar, P. Defence Tax Proposal Needs Modifications to Avoid Sending Wrong Signals, 26 February 2013. *Singapore Matters,* available online: http://singaporematters.blogspot.sg/2013/02/defence-tax-proposal-needs.html

Newspaper and Printing Presses Act (2002), Chapter 206, Singapore, available online: statutes.agc.gov.sg/

NEXUS *N.E.mation!8: Because You Played a Part,* 2013, available online: http://nemation.sg/

Nielsen (2011) *The Digital Media Habits and Attitudes of Southeast Asian Consumers* [White Paper], available online: http://static.slidesharecdn.com/swf/doc_player.swf?doc=201110nielsenseadigitalconsumerwhitepaperfinal-111107234448-phpapp01&stripped_title=nielsen-sea-digital-consumer-whitepaper&hostedIn=fb_feed

O'Reilly, T. What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Communications and Strategies,* 65, n._1 (2007), 17-37.

Ong, W. The Need for Engagement in Singapore's Defence Policies. *RSIS Commentaries,* 60 (2011), 1-2.

Osman, M.M. Speech by Senior Parliamentary Secretary for Defence and National Development Dr Mohamad Maliki Bin Osman at the Committee of Supply Debate 2012, *Parliamentary Statements,* 6 March 2012.

Republic of Singapore Navy *Sea of Support: Sending Inspiration Beyond Horizons,* 2012, available online: http://www.mindef.gov.sg/navy/careers/seaofsupport2012/

Rock Publicity *The State of Social Media in Singapore: The 2012 Rock Publicity Social Media Study,* available online: http://rockpublicity.com/wp-content/uploads/2012/11/2012-RP-SINGAPORE-SOCIAL-MEDIA-STUDY.pdf

Scheufele, D.A. and Tewksbury, D. Framing, Agenda-Setting, and Priming: The Evolution of Three Media Effects Models. *Journal of Communication,* 57, n._1 (2007), 9-20.

Spillman, K.R. Beyond Soldiers and Arms: The Swiss Model of Comprehensive Security Policy [conference paper]. *Stability and Change: Assessing Europe's Neutrals,* 19-21 November 1986, Washington DC: The Woodrow Wilson Center.

Storey, R.O. Singapore Military Uses Social Networking, 22 February 2011. *MIS Asia,* available online: http://www.mis-asia.com/resource/cloud-computing/singapore-military-uses-social-networking/?page=1

The Economist. Social Media in the 16th Century: How Luther went viral, 17 December 2011. *The Economist,* available online: http://www.economist.com/node/21541719

Wan, A. B*eing a Social Media Ambassador,* 23 August 2013, available online: http://ndru1.blogspot.sg/2013/08/being-social-media-ambassador.html

Wan, A. Should Women Serve National Service (NS) in Singapore?, 17 June 2013. *NDRU1,* available online: http://ndru1.blogspot.sg/2013/06/should-women-serve-national-service.html

ENDNOTES

1. S.B. Griffith, *Sun Tzu: The Art of War,* (London: Watkins Publishing, 2011), 124.
2. M. Mullen, JCS Speech. *NDU Conference on Military Professionalism,* 10 January 2011, (Washington DC: National Defense University), available online: http://www.jcs.mil/speech.aspx?id=1517
3. C.T. Goh, Speech by Mr Goh Chok Tong, Minister of Defence and Second Minister for Health, at the Official Opening of "The SAF Story Exhibition", *Singapore Government Press Release,* 5 January 1984.
4. K.R. Spillman, Beyond Soldiers and Arms: The Swiss Model of Comprehensive Security Policy [conference paper]. *Stability and Change: Assessing Europe's Neutrals,* 19-21 November 1986, (Washington DC: The Woodrow Wilson Center, 1987).
5. J. Frank, 'A Neutral's Perspective: The Role of the Austrian Armed Forces in Homeland Security' in J.L. Clark (Ed.) *Armies in Homeland Security: American and European Perspectives* (Washington DC: National Defence University Press, 2006), 119-148.
6. R. Matthews, and N.Z. Yan, Small Country 'Total Defence': A Case Study of Singapore. *Defence Studies,* 7, n._3 (2007), 376-395, 380-381.
7. Ministry of Education *Total Defence Day 2013,* 15 February 2013, available online: http://www.ne.edu.sg/files/Total%20Defence%20Day%202013.pdf, 5.
8. *Ibid.*, 2.
9. Ministry of Home Affairs *The Jemaah Islamiyah Arrests and the Threat of Terrorism* [White Paper], Cmd. 2 of 2003, (Singapore: MHA, 2003).
10. M.M. Osman, Speech by Senior Parliamentary Secretary for Defence and National Development Dr Mohamad Maliki Bin Osman at the Committee of Supply Debate 2012, Parliamentary Statements, 6 March 2012.
11. N. Carr, *The Shallows: What the Internet is Doing to Our Brains,* (New York: W.W. Norton & Company, 2010), 3.
12. N. Carr, Is Google Making us Stupid? *Yearbook of the National Society for the Study of Education,* 107, n._2 (2008), 89-94, 90.
13. M.E. McCombs, and D.L. Shaw, The Agenda-Setting Function of Mass Media. *Public Opinion Quarterly,* 36, n._2 (1972), 176-187.
14. D.A. Scheufele, and D. Tewksbury, Framing, Agenda-Setting, and Priming: The Evolution of Three Media Effects Models. J*ournal of Communication,* 57, n._1 (2007), 9-20.
15. D. Domke, D.V. Shah, and D.B. Wackman, Media Priming Effects: Accessibility, Association, and Activation. *International Journal of Public Opinion Research* 10, n._1 (1998), 51-74.
16. M. Castells, Communication, Power and Counter-power in the Network Society. *International Journal of Communication* 1, n._1 (2007), 238-266, p.241.
17. Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom,* (New Haven: Yale University Press, 2006), 179.
18. H.D. Lasswell, (2007) The structure and function of communication in society. *Journal of Communication Theory and Research,* 24 (Winter-Spring), 215-228, 223.
19. S.S. Lim, and E. Nekmat, 'Media Education in Singapore – New Media, New Literacies?' in C. Cheung (Ed.) *Media Education in Asia,* (Dordrecht: Springer, 2009), 185-197.
20. C. George, Freedom From The Press: Why The Media Are The Way They Are, 25 October 2001. *Air-Conditioned Nation,* available online: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN004067.pdf (accessed 18 April 2012).
21. Constitution of the Republic of Singapore, 1999, cited in J. Gomez, Restricting Free Speech: The Impact on Opposition Parties in Singapore. *The Copenhagen Journal of Asian Studies,* 23, n._1 (2006), 105-131, 106.
22. Newspaper and Printing Presses Act (2002), Chapter 206, Singapore, available online: statutes.agc.gov.sg/
23. Broadcasting Act (2012), Chapter 28, Singapore, available online: statutes.agc.gov.sg/
24. Cited in W. Bokhorst-Heng, Newspapers in Singapore: a mass ceremony in the imagining of the nation. *Media, Culture & Society,* 24, n._4 (2002), 559-569, 560.

25. Y. Ibrahim, Traditional and online media is the new normal [speech], Singapore Press Club Lunch, 23 April 2012. *MICA Press Releases and Speeches,* available online: http://app.mica.gov.sg/Default.aspx?tabid=79&ctl=Details&mid=540&ItemID=1393

26. B. Bimber, 'How Information Shapes Political Institutions' in D.A. Graber (Ed.) *Media Power in Politics* (Washington: CQ Press, 2011), 5-17, 16.

27. T. O'Reilly, What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Communications and Strategies,* 65, n._1 (2007), 17-37.

28. A.M. Kaplan, and M. Haenlein, Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons,* 53, n._1 (2010), 59-68.

29. Infographics.SG *Social Media Usage Statistics for Singapore,* 7 June 2013, available online: http://infographics.sg/?portfolio=social-media-usage-statistics-for-singapore-static-infographic

30. The Economist. Social Media in the 16th Century: How Luther went viral, 17 December 2011. *The Economist,* available online: http://www.economist.com/node/21541719

31. C. Li, and J. Bernoff, *Groundswell: winning in a world transformed by social technologies* [e-book], (Boston: Harvard Business Review Press, 2011), 40.

32. Cited in T. Chua, Singapore is one of the world's most evolved social media markets, 10 February 2011. *Singapore Business Review:* available online: http://sbr.com.sg/media-marketing/news/singapore-one-world%E2%80%99s-most-evolved-social-media-markets

33. S. Dutta, and I. Mia, *The Global Information Technology Report 2010-2011: Transformations 2.0,* (Geneva: World Economic Forum, 2011), 374.

34. Rock Publicity *The State of Social Media in Singapore: The 2012 Rock Publicity Social Media Study,* available online:http://rockpublicity.com/wp-content/uploads/2012/11/2012-RP-SINGAPORE-SOCIAL-MEDIA-STUDY.pdf, 23, 25 & 27.

35. Nielsen (2011) *The Digital Media Habits and Attitudes of Southeast Asian Consumers* [White Paper], available online: http://static.slidesharecdn.com/swf/doc_player.swf?doc=201110nielsenseadigitalconsumerwhitepaperfinal-111107234448-phpapp01&stripped_title=nielsen-sea-digital-consumer-whitepaper&hostedIn=fb_feed ,14.

36. *Ibid.,* 10.

37. T. Ahonen, Smartphone Penetration Rates by Country! We Have Good Data (finally), 12 December 2011. *Communities Dominate Brands,* available online: http://communities-dominate.blogs.com/brands/2011/12/smartphone-penetration-rates-by-country-we-have-good-data-finally.html

38. Cited in Chua, op. cit.

39. N. Fenton, 'Drowning or Waving? New Media, Journalism and Democracy' in N. Fenton (Ed.) *New Media, Old News,* (London: SAGE, 2010), 3-16.

40. W. Ong, The Need for Engagement in Singapore's Defence Policies. *RSIS Commentaries,* 60 (2011), 1-2.

41. D. Boey, Coming to terms with Singapore Armed Forces (SAF) Training Deaths, 6 April 2012. *Senang Diri,* available online: http://kementah.blogspot.sg/2012/04/coming-to-terms-with-singapore-armed.html

G. Lee, National Service - by Guest Spot Author Gordon Lee, 8 April 2011. *Rethinking the Rice Bowl: Tackling the Economic Questions as Singapore Transitions from Authoritarianism to Democracy,* available online: http://sonofadud.com/2011/04/08/ns/

42. Institute of Policy Studies (2000) *Citizens and the Nation - IPS Survey of National Pride and Citizens' Psychological Ties to the Nation* [press release], Singapore: Institute of Policy Studies, available online: http://lkyspp.nus.edu.sg/ips/wp-content/uploads/sites/2/2013/06/Press-Citizens-and-the-Nation-web.pdf

43. C-H. Leong, W.W. Yang, and M.W.H. Ho, (2013) *Singaporeans' Attitudes to National Service* [presentation slides], Singapore: Institute of Policy Studies, available online: http://lkyspp.nus.edu.sg/ips/wp-content/uploads/sites/2/2013/04/NS-study-8-Oct-2013_web.pdf

44. Hopmingu NS guy should have known better than to drink on train, 22 November 2013. STOMP, available online: http://singaporeseen.stomp.com.sg/singaporeseen/hey-goondus/ns-guy-should-have-known-better-than-to-drink-on-train-while-in-uniform

45. NEXUS *N.E.mation!8: Because You Played a Part,* 2013, available online: http://nemation.sg/

46. R.O. Storey, Singapore Military Uses Social Networking, 22 February 2011. *MIS Asia,* available online: http://www.mis-asia.com/resource/cloud-computing/singapore-military-uses-social-networking/?page=1

47. Republic of Singapore Navy *Sea of Support: Sending Inspiration Beyond Horizons,* 2012, available online: http://www.mindef.gov.sg/navy/careers/seaofsupport2012/

48. Ministry of Defence Public Affairs, *MINDEF/SAF Code of Conduct on Social Media Participation,* March 2013.

49. *Ibid.,* 6-11.

50. A. Wan, Should Women Serve National Service (NS) in Singapore?, 17 June 2013. *NDRU1,* available online: http://ndru1.blogspot.sg/2013/06/should-women-serve-national-service.html Muthhukumar, P. (2013) Defence Tax Proposal Needs Modifications to Avoid Sending Wrong Signals, 26 February 2013. Singapore Matters, available online: http://singaporematters.blogspot.sg/2013/02/defence-tax-proposal-needs.html

51. A. Wan, *Being a Social Media Ambassador,* 23 August 2013, available online: http://ndru1.blogspot.sg/2013/08/being-social-media-ambassador.html

CPT Lau Jian Sheng, Jason is currently attending the Introduction to Fighter Fundamentals pilot training course at Randolph Air Force Base, San Antonio, Texas. He is a recent distinguished graduate of the Specialised Undergraduate Pilot Training programme, which he completed at Laughlin Air Force Base, Del Rio, Texas. CPT Lau was a recipient of the SAF Overseas Scholarship in 2008. He holds a Bachelors of Arts (First Class Honours) in Sociology from the University of Warwick and a Masters of Philosophy in Modern Society and Global Transformations from the University of Cambridge.

Cyberspace: What are the Prospects for the SAF?

by **CPT Lim Guang He**

Abstract:

The development of cyberspace represents a rupture of security paradigms where state interests are being protected. Given the nature of cyberspace, the Singapore Armed Forces (SAF) faces challenges of interoperability at various levels. This essay discusses the prospects for elements which form the basis of the SAF cyber strategy framework by studying three pillars of action—Resilience, Deterrence and Interoperability. A cyber strategy must therefore also take into account three factors, i.e. environment, desired behaviours and actions. The purpose is to reconcile the offensive nature of cyber warfare with Singapore's defensive inclinations, while leaving sufficient ambiguity on a competent network to assure a maximum liberty of manoeuvre. As such, it is critical that the SAF rethinks its cyber architecture and maximises a spectrum of possible policy options for strategic interests, in order to win the battle of tomorrow.

Keywords: Resilience, Deterrence, Interoperability, Environment,

INTRODUCTION: NATIONAL STRATEGY VERSUS MILITARY STRATEGY

The awareness of the vulnerabilities of cyberspace for a state comes from its dependence on cyberspace for its administrative and industrial activity, the threat of destabilisation as a result of international cybercrime, spying, or sabotage, as well as from the wish to exploit the possibilities offered by cyberspace for its own good. Consequently, states have sought to develop specific civilian and/or military structures to add to the list of tools that complement the state's capacity to act on the international scene. If the cyber-attacks against Estonia in 2007 and Georgia in 2009 as well as the *Stuxnet* virus used against the Natanz nuclear enrichment facility in Iran in 2009 demonstrate how states are targeted directly in cyberspace, the phenomenon will only intensify with time. As the number of people with access to Information and Communications Technology (ICT) continue to increase and as societies continue to rely more and more on information systems, cyberspace's importance in the global security landscape can only gain further momentum.

The awareness of the vulnerabilities of cyberspace for a state comes from its dependence on cyberspace for its administrative and industrial activity, the threat of destabilisation as a result of international cybercrime, spying, or sabotage, as well as from the wish to exploit the possibilities offered by cyberspace for its own good.

To address this growing importance, states have responded with National Cyber Security Strategies (NCSS) which serve as a continuum across a wide array of objectives, notably cybercrime, cyber terrorism and cyber warfare. Singapore is no exception: the Information Development Authority of Singapore (IDA) and an ensemble of agencies execute Singapore's

NCSS under the umbrella of Infocomm security. As a major hub of economic activity, Singapore sees Infocomm security as a key to protecting investor confidence and instilling resilience in computerised activity. Naturally, a significant effort has been made in developing a coherent constellation of agencies. At its base, the IDA is the government agency responsible for implementing Information Technology (IT) security in the Government and Infocomm sectors, notably the objectives as spelled out in the Infocomm Masterplan Two since 2008 and now those from the National Cyber Security Masterplan 2018.[1] At the operational level, the Singapore Infocomm Technology Security Authority (SISTA)—a division within the Internal Security Department (ISD)—specialises in overseeing Singapore's IT security, particularly against cyber-terrorism and cyber-espionage, in coordination with other regulatory agencies.[2] SISTA also oversees the Critical Information Infrastructure Protection (CIIP) Programme which assists the Infocomm security efforts of critical infrastructure sectors.[3] At the executive level, the multi-agency National Infocomm Security Committee (NISC) directs and formulates national IT security policies. Meanwhile, the establishment of the INTERPOL Global Complex for Innovation (ICGI), a cybersecurity and cybercrime research facility which became operational in 2014 underlines Singapore's commitment to IT security and regulation.[4] Clearly, Singapore conducts a coherent NCSS to protect its core interests in cyberspace. The question is therefore: "Where does all this leave the Singapore Armed Forces (SAF)?"

The SAF is also aware of the opportunities and challenges of cyberspace, but the core of its strategy remains in warfighting.

The SAF is also aware of the opportunities and challenges of cyberspace, but the core of its strategy remains in warfighting. If the creation of the Cyber Defence Operations Hub in July 2013 bears witness to its growing commitment to cyber defence, it is but to defend MINDEF/SAF military networks against cyber threats. So is the SAF's cyber strategy as simple as that? This essay believes otherwise. The development of cyberspace represents a rupture of

Singapore Management University Wiki

Framework for Infocomm Masterplan 2 which depicts the vision, coverage, strategic outcome and the supporting strategic thrusts. Four strategic thrusts are identified to support attaining high resilience and availability of the Singapore's infocomm infrastructures.

security paradigms where the fundamental interests of the state can be attacked without the opening of hostilities in the physical world. Low-Intensity Cyber Conflicts (LICC) between states are already a reality on the international scene. In such cases, who is responsible for escalation in cases of riposte? Who can assure deterrence against other state cyber actors? If war is the continuation of politics by other means, and cyber defence is the prevention and the conduct of cyber war with defensive means, a NCSS is weakened without the armed forces.[5] There is as much importance attached to a credible military cyber strategy as there is to a robust NCSS.

Curiously, however, SAF literature on the subject remains largely undeveloped or subsumed under more generalised discussions. It appears that, despite the focus on a network-centric force in 3rd Generation (3G) transformations, the SAF's mission in cyberspace remains *a priori*. The central theme of this essay is therefore about encouraging deeper strategic thought on Singapore's place in the regional cyber competition and eventually the SAF's approach to cyberspace as a whole. We begin first by examining the notions of cyberspace and how they relate to cyber strategy. We then attempt to construct a prospective for the SAF's cyber strategy framework and seek to define an approach to a military cyber strategy adapted to Singapore's needs for the near future. Finally, we will reflect on how the SAF can take advantage of its circumstances to pursue policies favourable to maximising the range of cyber policies in the long term. In essence, we want to identify the rules of the game in the local perspective and pre-empt their transformations in the near future.

MAKING SENSE OF CYBER STRATEGY AND CYBERSPACE

Like the terms 'security' and 'defence', the term 'cyberspace' finds itself victim to a myriad of interpretations, each dependant on the context in which they are defined. The American definition of cyberspace as *"a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"* is one such interpretation.[6] However, Daniel Ventre and Charles Préaux[7] highlight that the notion of "a global domain within the information environment" raises two questions: Firstly, if cyberspace is within or distinct from the information environment, and secondly, what is the resolution between the electromagnetic spectrum and cyberspace?[8] Moreover, in the context of armed forces, should electronic warfare units be integrated into cyber operations?

Instead, Ventre divides cyberspace into three different layers: bottom (physical and material), medium (application and software), and high (psycho-cognitive) (See *Table 1*).[9] In this manner, we perceive cyberspace not as a singular entity but a combination of parallel entities relying on one another. Going back to the first question asked earlier—that is, if cyberspace is within or distinct from the information environment—we note that the answer is both yes and no. The high and medium layers of cyberspace are established within the non-physical information environment—which we can call the 'autonomous cyberspace', but the bottom layer relates to the physical electromagnetic environment. We therefore choose to define cyberspace based on how much overlap we perceive from the bottom layer. While 'autonomous cyberspace' represents a novel battle space in the information environment, it is insufficient to treat cyberspace as a separate battle space because it can never be truly autonomous.

To answer the second question—what is the resolution between the electromagnetic spectrum and cyberspace—since all three layers are intimately related to one another, the resolution between the electromagnetic spectrum and cyberspace depends on how this overlap is interpreted in action. Consequently, we apply the notions of cyber defence, cyber conflicts, cybercrime and cyber security by observing the dialectic between the characteristics of each cyberspace layer, the type of attacks, the profile

	CHARACTERISTICS	POSSIBLE FORMS OF ATTACK
HIGH LAYER	Psycho-cognitive	Cognitive hacking: modification of screen displays, disfiguration of websites, propaganda operations...
MEDIUM LAYER	Applications, software, code, data, protocols, norms	Hacking, Viruses, Backdoors, Trojans...
BOTTOM LAYER	Material, hardware, cables, satellites, computers, communication infrastructure	Cutting of submarine communications cables, satellite destruction or disruption, physical destruction of terrestrial communication infrastructure, signal jamming or interception, EMP attacks...

Table 1: Association of each cyberspace layer with the possible forms of attack.

of the actors, and in the case of the military, the point or points of intersection with conventional spaces (air, land, sea, and space).[10]

These observations lead us to Hervé Coutau-Bégarie's vision of cyber strategy in *Traité de Stratégie*.[11] According to Coutau-Bégarie, classical strategy offers direct applications across three physical spaces: land, sea, and air (or aerospace). As technological progress changes how we fight across these three physical spaces, we have also constructed a nonphysical battle space in which conflicts can exist. This battle space was first considered as the electromagnetic dimension and subsequently the information dimension and cyberspace was considered a part of these dimensions.[12] Over time, however, cyberspace has become more and more distinct from these dimensions. Coutau-Bégarie believes that the point of rupture in strategic thought therefore occurs when cyberspace is 'autonomous' enough to be treated as a separate space, but it is still too early to do so.[13] Conceiving a cyber-strategy is to consider the preparation and the use of force in a specific environment (that is, cyberspace), even if the environment overlaps heavily with the information environment, forcing us to rethink other strategies. Cyberspace is never autonomous, nor should cyber strategy be. With this in mind, Bertrand Boyer defines cyber strategy as "the study of the principles and the modalities of conflict in, by, and for cyberspace."[14]

Yet cyber strategy is not the same for everyone. The cyber competition between states is characterised by an asymmetric balance of power.[15] As Richard Clarke points out, the most digitally and technically advanced state is one that is also the most vulnerable and fragile – its cyber architecture is practically indefensible.[16] The same can be said for states on the other end of the spectrum – states which are the least dependent on cyberspace have the least to lose. Seen in this manner, the problem for cyber powers is therefore about reducing vulnerability without reducing power. But we can also argue the other way round: the less dependent states are also the easiest ones to defeat in cyberspace since there are far less targets and are generally less secure. However, the low dependence itself presents a low utility of cyber-attacks and such targets often have methods to respond against more powerful cyber actors. Seen in this manner, the problem for cyber powers is about the effects desired via a cyber-manoeuvre. Although it is more difficult to defend a complex system, it is also more difficult to really bring one down, and vice-versa.

According to Ventre, we can define eight categories of actors based on three criteria: offensive capacity, defensive capacity and complexity/dependence (see

CATEGORY	OFFENSIVE CAPACITY	COMPLEXITY / DEPENDENCE	DEFENSIVE CAPACITY
A	Strong (+)	Strong (+)	Strong (+)
B	Strong (+)	Strong (+)	Weak(-)
C	Strong (+)	Weak(-)	Strong (+)
D	Strong (+)	Weak(-)	Weak(-)
E	Weak(-)	Strong (+)	Strong (+)
F	Weak(-)	Strong (+)	Weak(-)
G	Weak(-)	Weak(-)	Strong (+)
H	Weak(-)	Weak(-)	Weak(-)

Table 2: Categories of state cyber actors based on three criteria.

Table 2).[17] As an example, in category A we have the United States (US), while in category H we have the least connected states. Most state cyber actors occupy the spectrum between categories E and F, with a few exceptions. China can be regarded as a borderline category C due to its strict regulation of cyberspace; states such as Syria and Pakistan can be considered between category D and H due to beliefs about their offensive cyber capabilities. Clearly, while a state in category A might seem to be in a position of dominance, it is rather a state in category D which is advantaged. Such a representation of categories and asymmetry is not to simplify the cyber competition but to highlight that the competition is not one-dimensional—states can and will pursue different cyber strategies according to their circumstances. Not everyone is looking to become a category A or C. As states become more and more invested in cyberspace, changes in the relationship between different categories of cyber actors will also affect the security landscape of the region as a whole. A cyber strategy must therefore also take into account the environment of the actor, how the actor wants to behave in the environment and actions which can help shape the environment to its advantage.

PROSPECTIVE FOR THE SAF'S CYBER STRATEGY FRAMEWORK

For the SAF, we first echo our last observation of cyber strategy by defining Singapore's cyberspace

ENVIRONMENT	• Asia is a hotspot for cyber criminality, cyber espionage, and low intensit`y cyber conflicts • There is growing interstate competition in cyberspace • Lack of regional momentum in judicial and regulatory practices • Offensive cyber capabilities are likely to proliferate in the future
DESIRED BEHAVIOUR	• Minimize the threat of cyber-attacks against Singapore • Policies favourable to prosperity and regional stability • Cyber capabilities are for defensive purposes
ACTIONS	• Prudent exploitation of cyberspace for military applications • Encouragement of regional cooperation • Study of legislative possibilities

Table 3: Singapore's environment, desired behaviour and actions in cyberspace.[18]

environment, her desired behaviour and the actions associated (see Table 3). Looking at the links between these three elements and the abovementioned layers of cyberspace proposed by Ventre, we identify areas where the armed forces can intervene with or without the Infocomm security umbrella. We then consider the continuum of policies which the SAF can adopt in order to address these areas. This essay does not pretend to present a comprehensive cyber strategy framework for the SAF as such an effort is beyond its depth. Instead, we prospect for elements which form the basis of the SAF's cyber strategy framework by looking at three pillars of action:

THE FIRST PILLAR: RESILIENCE

For the SAF, the most important element of its cyber strategy is the security of its information systems. As *Table 1* implies, there are three aspects. At the bottom layer, the technical progress promised by 3G transformation to relieve the effects of Clausewitzian 'fog' and 'friction' is counterbalanced by an increased vulnerability from a dependence on information systems and interconnectivity. In order to realise its networking and sense making objectives,

Minister Chan Chun Sing announcing the commissioning of the WAC system using the system itself via a handset hooked up to the D-TCS in the background.

the 3G SAF development strategy predicts the necessity of Commercial-Off-The-Shelf/Modifiable-Off-The-Shelf (COTS/MOTS) solutions from commercial ICT to deliver broadband to the lowest denominator on the ground.[19] Developments such as the Changi C2 Centre in 2009 and the upgrading of the Army's Wide Area Communications (WAC) system with D-TCS broadband network in 2013 further illustrate this trend.[20] Since these solutions reveal to be the critical frameworks of our warfighting capabilities tomorrow, experiences from *Stuxnet* and *Flame* reiterate the importance of careful procurement and a significant attention on behalf of the local defence research agencies.

At the same time, the SAF's technological edge presents its own set of challenges in managing the integrity and availability of the communication systems between its different military networks. This means preparing for scenarios such as physical attacks against server locations, prolonged electrical outages, and operating in a degraded network environment. This may be the less glamorous part of a network-centric force, but it is imperative to a credible 3G SAF.

At the middle layer, cyber defence start from the enforcement of measures as simple as the use of up-to-date anti-virus programmes and the systematic removal of malicious attachments from the Internet. The core value 'safety' is also present in cyberspace and every user in the SAF is an actor of cyber defence. Furthermore, this essay believes that with the growing interaction between military and civilian networks, there is real interest in reviewing the SAF's responses against cyber intrusions while ensuring minimal disruption to normal workflow. Also, finding the necessary competencies to maintain this expertise in a sector where expertise are rare and sought after, particularly in the private sector, represents a real challenge.[21] For human resource planners, the SAF must stay competitive to attract and retain cyber defence experts.

At the high layer, the SAF is presented with a different set of challenges. Firstly, all its portals

on the internet are subject to incessant intrusion attempts. Apart from the obvious necessity of keeping them operational, the protection of these portals serve the mission to safeguard the image of the SAF as a credible force. In this manner, the defacement of several government websites involving the Anonymous hackitivist group in October and November 2013 is a timely reminder of this imminent threat.[22] Secondly, it is not uncommon for units to set up their own communities on social networks such as Facebook and Twitter for cohesion purposes. While we can expect such initiatives to be self-regulated on the basis of command guidance, the risk of an inadvertent release of sensitive information cannot be discounted. Even if this is not the case, hackers can obtain valuable information from such communities via social engineering in order to produce significant intelligence. The SAF must therefore continue to reinforce measures to ensure proper handling of information by such communities over the Internet, or even develop processes to assure the rapid detection and treatment of incidents.

THE SECOND PILLAR: DETERRENCE

Deterrence is also relevant in cyberspace. In tandem with national policies, the SAF has also invested to attain the resources and the capability for cyber defence. However, it does not share the same circumstances as its civilian counterparts. While it may assist in the intervention of criminal or delinquent incursions under the umbrella of Infocomm security, those are not its primary objectives. Its main concern is national defence and security. However, so far the dialogue has only been about the cyber defence of military networks. Returning to the themes of acceptability and symbolism, what form of escalation policy does the SAF provide in case of a state-sanctioned cyber-attack? Going back to the definitions of a just war, how should the SAF respond? Even the US' reservation of the right to retaliate against a cyber-attack with military force remains ambiguous when coupled with the dialogue of "all necessary means – diplomatic, informational, military and economic."[23]

More specifically, the SAF is interested in deterring strategic cyber-attacks which target critical national infrastructure or High-Impact Cyber Conflicts (HICC). Although inter-state tensions in cyberspace today rarely exceed LICC which are "aimed towards influencing or shaping public opinion" (e.g. between the Philippines and China in 2012) and are likely to remain as such in the future, the scale of disruption experienced by critical systems in Estonia during the cyber-attacks of 2007 demonstrate the relevance of HICC.[24] At the same time, the phenomenon of Advanced Persistent Threats (APT) as a form of continuous and coordinated attacks against state and business organisations is likely to expand in the future. Clearly, there is reason to want to deter cyber-attacks from the strategic interests of the state. However, the challenge lies in distinguishing the concept of deterrence in cyberspace from the current SAF discourse on deterrence. Kenneth Geers[25] examines two options available—denial and punishment—and invoke the notion of 'mutually assured disruption' as a possible strategy.[26] Nevertheless, there are real operational and judiciary difficulties involved. Deterrence may be enhanced by conducting or demonstrating the capacity to conduct offensive cyber operations against a potential or alleged cyber adversary, but it also presents a new set of problems which we will discuss later. Here, we focus on the problem of qualification: attacks may be perpetrated by actors who do not belong to any armed forces, while targets may serve both civilian and military purposes. While the principles of International Humanitarian Law (IHL) apply to cyber-attacks in the context of armed conflict, in reality it is very complex to establish the attribution of a cyber-attack to a state.[27] To cater for this, the SAF must consider a range of options with different levels of elaboration for different circumstances, even going as far as to achieve an element of surprise. In terms of credibility, the SAF must also consider the level of transparency it wishes to project when communicating about its activities involving cyberspace and its responses against alleged cyber aggressors. Lastly, while it is logical to entrust peacetime cyber defence in the hands of the IDA and the SISTA, there may a

need to review the SAF's involvement in government responses against different types of cyber threats as indicated in Table 1.

THE THIRD PILLAR: INTEROPERABILITY

Given the nature of cyberspace, the SAF faces challenges of interoperability at various levels. The first comes from the necessity of coordinating the nodes of cyber capabilities across the SAF. For small armed forces, missions such as Cyber Intelligence (CYBERINT) operations require extensive resources and coordination to produce significant output. Another constraint comes from the cost and difficulty of training sufficient numbers of personnel and of maintaining state-of-art equipment for each service. Such investments only yield returns in the long run and technologies superior to existing architecture often become available within a few years. To maintain its technological edge while ensuring financial prudence, the SAF must strive to develop its cyber capabilities in a centralised and joint manner. In this regard, Commander of the US Cyber Command, General Keith B. Alexander, has called for a 'cyberteam' approach based on the convergence of the signal and cyber communities due to their overlaps, as well as the standardisation of training for information specialists across different services, forming a "a series of career fields all together."[28] Likewise, the SAF can explore the concept of 'cyberteam' by studying how signals and intelligence vocations of each service can pool their resources together to optimise the development and transfer of cyber expertise among one another.

The second challenge follows up with the necessity of a whole-of-government approach to cyber defence, as illustrated by the $130 million programme into cybersecurity research announced in October 2013 involving the National Research Foundation (NRF), the Ministry of Defence (MINDEF), the Ministry of Home Affairs and the National Security Coordination Secretariat.[29] Likewise, while the outline of the SAF's Cyber Defence Operations Hub in June 2013 appears to be restricted to military objectives, its partnership with SISTA to track cyber trends suggests a greater field of action.[30] The problem, however, lies in the task of implementing an effective doctrine of employment. Clearly, MINDEF should continue to collaborate with other ministries and agencies to maximise the exploitation of information available in cyberspace. At the same time, there is a need to review the policies and modes of action against different levels of cyber-attacks: what kind of inter-ministerial optimisation should we be pursuing to achieve the shortest Observe, Orient, Decide, and Act (OODA) loop in the event of a massive and unrestricted cyber-attack?

Finally, we move on to the realm of international cooperation. In South East Asia, the lack of regional momentum in judicial and regulatory practices is likely to increase the odds of miscalculation and misunderstanding between states. Caitríona H. Heinl[31] points out that despite its growing importance, cyber security remains ambiguous in official accounts by the Association of South East Asian Nations (ASEAN) in 2013 and a regional framework is far from taking off.[32] Singapore's Prime Minister, Lee Hsien Loong's call for ASEAN to "strengthen our defences and cooperate to deal with these common [cyber] threats" in the aftermath of cyber-attacks against Singapore, Thailand, and the Philippines in November 2013 indicates that the issue is likely to warrant greater scrutiny in the future, but the question is how?[33] Heinl's suggestion that member states of ASEAN establish a 'no-use zone' by agreeing to not use offensive cyber capabilities in the region is a possibility consistent with the organisation's ethos of confidence building and preventive diplomacy, although from a realist perspective the proliferation and cross-border nature of cyber threats, state-sponsored or otherwise, may condemn such an initiative to irrelevance.[34] Instead, ASEAN might find common ground by unifying to address their fundamental challenges. Since regional and international cooperation is essential to effective action against cyber threats and to diffuse mistrust, the SAF should be actively exploring ways with its means to aid the process. Even though interoperability with other armed forces in the cyber domain is neither realistic nor the objective of the SAF, it can and should

pursue policies to encourage confidence building and sustained communication with its regional counterparts in cyber defence as a form of hedging against cyber competition in Southeast Asia.

WHAT ABOUT OFFENCE?

For the SAF, Weng Zai Shan's assertion that "the development of offensive cyber capabilities will add to effectiveness of the military" is highly debatable.[35] If the doctrine, challenges, and the current organisation of the SAF indicate an elevation in cyber defence capabilities, the conduct of offensive operations in cyberspace remains infinitely complicated. An institutional cyber-attack competence is very different from an individual cyber-attack competence; to do so requires sustained investment into technical means to obtain accurate, day-to-day information on systems of potential adversaries, as well as an industrial and technological base backed by a range of uncommon skills to develop an effective 'cyber-arsenal'. Moreover, we do not have sufficient examples of "large scale, state-sanctioned [cyber] attacks" and have to rely on theories to understand the utilisation of cyber-weapons.[36] Given the uncertainties and risks involved, the perceived 'force multiplier' potential of cyber operations remains uncertain in the near future.

While the abovementioned prospective points toward greater military participation in cyberspace, there is a catch: as Singapore is highly dependent on cyberspace but suffers from little geostrategic depth, its core interests in the domain are best expressed by assuring defence rather than menacing attack or retaliation.

Yet the biggest obstacle is far from technical. Malaysia's summoning of High Commissioner Ong Keng Yong to its foreign ministry in November 2013 following allegations of Singaporean assistance to a US-led spying network in Asia forebodes the diplomatic repercussions of cyber incursions in our region.[37] One may argue that, as was the case for Brazil and Germany's strong criticism of US spying on their networks in 2012, this is only natural, but for a small country like Singapore, an intrusive cyber capability is just one Edward Snowden away from a ticket to diplomatic catastrophe. If the purpose is to enhance deterrence, an offensive cyber capacity in the near future is likely to be cost-ineffective for the SAF, and even diplomatically counterproductive.

DEFINING SAF'S VISION OF AN 'INDIRECT' CYBER STRATEGY

While the abovementioned prospective points toward greater military participation in cyberspace, there is a catch: as Singapore is highly dependent on cyberspace but suffers from little geostrategic depth, its core interests in the domain are best expressed by assuring defence rather than menacing attack or retaliation. Contrary to its forward defence posture, Singapore is not trying to punch above its weight in terms of offensive cyber capabilities. To do so, this essay believes that the SAF can do well by restricting its current dialogue of cyber warfare to information warfare—the protection of information and networks from an adversary, the careful use of disinformation, and operations to prevent potential adversaries from doing the same. The objective of cyber operations is to achieve the domination of information on the battlefield, as opposed to inflicting physical effects on an adversary. In this manner, the SAF's main missions in cyberspace should be to (1) ensure the performance, integrity and security of its network infrastructure; (2) provide the necessary assistance to protect the electronic systems of Singapore's critical infrastructure; (3) seeking new and innovative ways to exploit cyberspace for military applications; and (4) help foster national, regional and global cooperation in cyberspace. The purpose is to reconcile the offensive nature of cyber warfare with Singapore's defensive inclinations, while leaving sufficient ambiguity to assure a maximum liberty of manoeuvre.

In reality, it is critical that the SAF rethinks its cyber architecture and spending based on rules and procedures for a flexible posture in the long term. The more pressing concern at the moment is about developing new policies of exploiting cyberspace in existing architecture for signals intelligence and information warfare. As both the SAF and the nature of cyberspace evolve, there is merit in studying a spectrum of possible policy options to protect her own strategic interests.

PREPARING FOR THE FUTURE

One of the ways the SAF can contribute to the national cyber defence strategy is to look into the potential of the recently set up SAF Volunteer Corps. In France, the *Réserve Citoyenne Cyberdéfense* (Cyber Defence Citizen Reserve) network, launched in September 2012, comprises of volunteers who work or who are interested in the domain of cyber defence/ cyber security and would like to share their expertise for the benefit of the network, as well as other civilian members who wish to share their expertise in the network's work groups.[38] In the United Kingdom, a similar effort has been undertaken with the formation of the Joint Forces Cyber Group in May 2013.[39] This essay believes that the SAF venture's into the volunteer scheme programme can extend from such an initiative to develop a reserve capable of supporting the national effort in the event of a major cyber crisis.

At the operational level, Singapore should be looking into refining options for a coordinated response against cyber-attacks by preparing for government-wide exercises against simulated cyber threats. For example, the coordinated execution of Exercise Highcrest in 2013 between the MINDEF and the MHA to test the government's response to simulated terrorist threats and to validate the National Maritime Security System (NMSS) can be built upon to explore similar opportunities in cyberspace. From information sharing to fire-fighting operations, its engagement of over 1,600 personnel from 20 agencies represents the complexity and span of activities which a cyber-attack against Singapore's critical infrastructure may require.[40] Likewise, the SAF should be pursuing similar exercises to test the resilience of its own networks and its capability to operate at various levels of network degradation.

In the longer term, Singapore must look at leveraging its educated population to create an environment and a mass of specialists who will serve as the foundations for national cyber defence. Activities such as the organisation of the National Infocomm Competition since 2012 to raise the exposure of students in the domain of Infocomm, or the Defence Science and Technology Agency's (DSTA) organisation of a learning camp for tertiary students "to promote cyber security interest among youths" in December 2013, can be conducted in a coordinated and progressive manner with MINDEF to help cultivate Singapore's next generation of cyber warriors.[41] Interestingly, Israel's technology sector offers an example of how the SAF can contribute to this effort. Today, Tel-Aviv claims the highest density of high-tech startups in the world—earning it the nickname Silicon Wadi—and is widely recognised as one of the world's best cities for high-tech startup entrepreneurs. Less known is the fact that the Israel Defence Forces (IDF) serves as the breeding ground for many of them: recruits posted to technical support units are put through an intensive six-month computer training course which teaches "programming skills, teamwork, project management, and [most importantly] creativity."[42] Coupled with the IDF's policy of providing funding and resources to encourage entrepreneurship in military projects, the IDF has played an important role in forming Israel's start-up companies. Today, numerous Israeli firms specialising in cyber-related solutions from web security to big data storage are all part of the industrial and research base for the country's cyber readiness strategy.

For the SAF, the Israeli example offers insight into how we can maximise the potential of National Service for Generation Y while addressing future threats. Clearly, the Productivity and Innovation Effort (PRIDE) movement to make MINDEF a learning organisation

that continuously seeks innovation and improvement is a good starting point; the objective of such an initiative can be extended to the empowerment of our NSmen balanced with real military applications. However, the task is far from the SAF's own. Looking at the larger picture, there is merit into looking at how MINDEF and other national agencies can work together on a greater scale and with a coherent cyber policy to encourage youth participation and entrepreneurship in cyber-related solutions—which will pay dividends in the long run. If Singapore's ambitions include establishing itself as the Silicon Valley of the region, the SAF is a potential actor in both supporting and benefitting from the trend.

The SAF, in its capacity, can contribute to the ASEAN's ethos of confidence-building by spearheading efforts to collaborate with other armed forces in the region, depending on the degree of interest and the level of mutual trust. For instance, Singapore's experience from hosting the Pacific Endeavour series of annual multi-national communication interoperability exercises can serve as inspiration for further collaborations with regional partners. The usage of an 'exercise network' during such instances can also be improved upon to establish a persistent testing ground for operational tests—in which simulations can be run in order to validate concepts, systems, or processes pertaining to cyber defence.

CONCLUSION

It is likely that victory for any military engagement tomorrow will not only require mastery of the physical battlefield, but also the points of intersection with cyberspace. For the SAF, these intersections represent both vulnerabilities as well as opportunities brought forth by 3G transformation. Moreover, the phenomenon of cyber-pervasiveness is not restricted to the battlefield: 'cyber-peace' simply does not exist. We are faced with a threat that is multiform, permanent and sinister, and it is only going to get worse. This essay has so far demonstrated how the SAF's cyber strategy must also take into account the different layers of cyberspace to address diverse concerns in daily operations, but the real difficulty lies in the specifics: what is the SAF's brand of 'deterrence and diplomacy' in the event of cyber conflicts? How will the SAF's cyber capabilities evolve along with Infocomm security? Although the doctrine and organisation of the SAF's operations in cyberspace have yet to mature, the need to regularly prospect for changes to its approach to cyberspace will only become more apparent as time goes on.

ENDNOTES

1. *Ministry of Home Affairs,* "Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats", 1 October 2009, http://www.mha.gov.sg/news_details.aspx?nid=MTU2MQ%3D%3D-0tPkaml9VAY%3D.
2. Ibid.
3. Masagos Zulkifli, "Opening Address to 22nd GovernmentWare Conference at Suntec Singapore International Convention & Exhibition Centre", https://www.mha.gov.sg/news_details.aspx?nid=Mjk2OQ%3D%3D-VO8owVZQ3SA%3D.
4. The INTERPOL Global Complex for Innovation, http://www.interpol.int.
5. Bertrand Boyer. *Cyberstratégie: l'Art de la Guerre Numérique*, (Paris: Nuvis, 2012), 21-24.
6. *Joint Chiefs of Staff,* JP 3-13: Information Operations, Department of Defense, United States, 27 November 2012, 30.
7. Daniel Ventre is a Researcher at the CNRS (French National Centre for Scientific Research) while Charles Préaux is a Professor, founder and principal of the School of Engineering in Cyber Defence, National School of Engineers, South Brittany, France.
8. Daniel Ventre and Charles Préaux, "Que couvrent les dénominations cybers liées à la défense?", *Défense & Sécurité Internationale,* no. 32 (2013), 9, own translation.
9. Ibid.
10. Daniel Ventre, *Cyberespace et acteurs du cyberconflit,* (Paris: Hermès Lavoisier, 2011), 87-88.

11. Hervé Coutau-Bégarie was a Research Director of Strategy at the War College (EdG), President of the French Commission of Military History , Professor at the top of Staff Course (CSEM), Director of studies at the Ecole Pratique des Hautes Studies and a Professor at the Catholic Institute of Higher Studies .

12. Hervé Coutau-Bégarie, *Traité de Stratégie,* 7th ed. (Paris: Economica, 2011), 488-490.

13. Ibid.

14. Bertrand Boyer. *Cyberstratégie: l'Art de la Guerre Numérique,* (Paris: Nuvis, 2012), 27-28.

15. Daniel Ventre, *Cyberespace et acteurs du cyberconflit,* (Paris: Hermès Lavoisier, 2011), 142.

16. Clarke R., Knake R., *Cyber War: The Next Threat to National Security and what to do about it,* (New York: Ecco, 2010), 136-137.

17. Daniel Ventre, *Cyberespace et acteurs du cyberconflit,* (Paris: Hermès Lavoisier, 2011), 143.

18. James Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia", Prepared for the Lowy Institute MacArthur Asia Security Project, *CSIS,* 07 March 2013.

19. IKC2 for the ONE SAF: Building the 3rd Spiral, 3rd Generation SAF, *POINTER* Monograph, n.o.5 (2008), 16.

20. Sheena Tan. "Battlefield info-sharing goes digital." *Cyberpioneer,* 10 May 2013.

    http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2013/may/10may13_news2.html.

21. Grace Chng, "Singapore's cyber defence firepower gets $130m boost", *The Straits Times,* 28 Oct 2013, http://news.asiaone.com/news/singapore/singapores-cyber-defence-firepower-gets-130m-boost.

22. Irene Tham, "Singapore government agencies on alert after hackers threaten attacks", *The Straits Times,* 1 November 2013, http://www.stasiareport.com/the-big-story/asia-report/singapore/story/singapore-government-agencies-alert-after-hackers-threaten.

23. "U.S. International Strategy for Cyberspace", *The White House,* 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf.

24. Miguel Alberto N. Gomez, "Awakening the Cyber Dragon: China's cyber strategy and its impact on ASEAN", The Second International Conference on Cyber Security, *Cyber Peacefare and Digital Forensic,* 2013, 254-256.

25. Kenneth Geers is an analyst based in Kiev, Ukraine. He was the first US Representative to the NATO Cooperative Cyber Defence Centre of Excellence in Estonia and the author of *Strategic Cyber Security,* Editor of *The Virtual Battlefield: Perspectives on Cyber Warfare,* Technical Expert for the Tallinn Manual on the *International Law Applicable to Cyber Warfare,* and author of more than twenty articles and chapters on cyber conflict.

26. Kenneth Geers. "The Challenge of Cyber Attack Deterrence", *Computer Law & Security Review* 26, no.3 (2010), 300-303.

27. Ronan Doaré, Oriane Barat-Giniès, and Éric Pomès, "Les cadres juridiques nationaux et internationaux du cyberespace", *Défense & Sécurité Internationale,* no.32 (2013), 57-58.

28. Robert K. Ackerman, "Cyber Command Redefines the Art", *Signal Magazine,* 1 June 2013, http:// www.afcea.org/content/?q=node/11117.

29. Grace Chng, "Singapore's cyber defence firepower gets $130m boost", *The Straits Times,* 28 Oct 2013, http://news.asiaone.com/news/singapore/singapores-cyber-defence-firepower-gets-130m-boost.

30. "Singapore unit to target hackers", *The Straits Times,* 2 July 2013

    http://www.nationmultimedia.com/ aec/Spore-unit-to-target-hackers-30209479.html.

31. Caitríona H. Heinl is a Research Fellow responsible for research on cybersecurity matters under the Homeland Defence Programme at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). CENS is a research unit which works closely with the National Security Coordination Secretariat (NSCS) within the Prime Minister's Office, Singapore.

32. Caitríona H. Heinl, *Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime,* S. Rajaratnam School of International Studies, 9 September 2013, 2-3.

33. Irene Tham. "PM Lee: Asean nations must work together to combat cyber threats", *The Straits Times,* 14 November 2013, http://www.straitstimes.com/breaking-news/singapore/story/pm-lee-asean-nations-must-work-together-combat-cyber-threats-20131114.

34. Caitríona H. Heinl, "Tackling Cyber Threats: ASEAN Involvement in International Cooperation", *RSIS Commentaries,* no. 114 (2013), 21 June 2013.http://www.rsis.edu.sg/publications/Perspective/RSIS1142013.pdf.

35. Weng Zai Shan "Defence in the Cyber Domain", *POINTER* 39, n.o.4 (2013), 40.

36. Ross M. Rustici, "Cyberweapons: Leveling the International Playing Field", *Parameters* 41, n._3 (Autumn 2011), 32.

37. Boo Su-Lyn, "Call in Singapore, PKR tells Putrajaya as spy row grows", *Malay Mail Online,* 25 November 2013, http://www.themalaymailonline.com/malaysia/article/call-in-singapore-pkr-tells-putrajaya-as-spy-row-grows.

38. "Le réseau de la réserve citoyenne cyberdéfense", *France Ministry of Defence,* 26 February 2014, http://www.defense.gouv.fr/reserves/presentation/cyberdefense/le-reseau-de-la-reserve-citoyenne-cyberdefense.

39. "Working for Joint Forces Command", *UK Ministry of Defence,* https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment.

40. "Whole-of-Government Response to Simulated Terrorist Threats at Exercise Highcrest 2013", *MINDEF official release,* 6 Nov 2013.http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2013/nov/06nov13_nr2.html.

41. "National Infocomm Competition", *Infocomm Development Authority of Singapore.*

    http://www.ida.gov.sg/Collaboration-and-Initiatives/Initiatives/Store/National-Infocomm-Competition-NIC.; "Cyber Defenders Discovery Camp", *Defence Science & Technology Agency,* http://www.dsta.gov.sg/cyber-defenders.

42. Mathew Kalman, "Israel: Boot camp for start-up success", *BBC,* 11 September 2013,http://www.bbc.com/future/story/20130911-israel-military-key-to-start-ups.

CPT Lim Guang He is currently an Air Traffic Controller in 203 SQN, Air Surveillance and Control Group. He holds a Masters of Engineering from the French Air Force Academy and a Masters of Science and Technology from the University of Aix-Marseille.

How a Good Offence is not the Best Defence: An Analysis of SAF's Approach to Cyber Warfare

by **LTA Ng Yeow Choon**

Abstract:

Technological advancement has ushered in an era of network-centric warfare where cyberspace plays an instrumental role in military operations. Due to its integral nature to modern militaries, cyberspace offers the ideal platform on which military operators can conduct their missions. Cyber warfare refers to the military doctrines and tactics used by operators in their attempt to gain dominance in the realm of cyberspace. Through the analysis of the offensive and the defensive aspects of cyber warfare, this paper argues that the SAF should invest in cyber-defence rather than cyber-offence. In addition, it suggests that by focusing on cyber-defence, the SAF may not only deter potential military aggressions from state actors but also protect Singapore's civilian infrastructure and institutions from non-state entities.

Keywords: Network-centric Warfare, Technology, Cyber Defence, Deterrence

INTRODUCTION:

Improvements in information technology and the evolution of business organisations have prompted militaries around the world to adopt new processes and take advantage of innovations. Among these innovations, increased connectivity between computer systems and effective coordination across multiple platforms have allowed modern militaries to employ systems holistically instead of individually—a fundamental shift from platform-centric warfare to network-centric warfare.[1]

NETWORK-CENTRIC WARFARE AND CYBERSPACE

The SAF, like other modern militaries in the world, underwent its 3rd Generation Transformation and established itself as a network-centric force.[2] A network-centric force is characterised by two broad themes. First, it involves a shift in focus from the weapons platform, such as the battle tank or the submarine, to the information network. Second, it emphasises a holistic employment of military systems in a dynamic battle environment over deployment by individual military units.[3] The advent of network-centric warfare revolves around the usage of interconnected computer systems and military platforms—every component of network-centric warfare occurs within the sphere of cyberspace. Cyberspace, succinctly defined by the United States (US) Department of Defense, is *"the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*[4] The more a military identifies itself as a network-centric force, the more connected it is to the cyberspace.

While network-centric warfare offers the obvious advantage of incorporating technology and sound organisation as force multipliers, the accompanying connectedness with cyberspace presents some vulnerability.

A network-centric force is susceptible to disruptions to its command and control mechanism. The enemy can disable key components of a network-

centric force, preventing commanders from issuing orders, units from communicating with one another, or even individual weapon systems from sharing essential information. It is the defence against such cyber-attacks that spurs network-centric militaries to establish teams of cyber experts. The US Cyber Command and the 'Chinese Information Support (Assurance) Base' were established to cope with the realities of this new realm of warfare.[5] These new military units are responsible for doctrines and tactics regarding cyberspace—developing cyber weapons and carrying out cyber-offence operations, while preventing their opponents from doing the same.[6]

Being a small city-state, Singapore has no illusions about the state of the region or the world.[7] Taking cues from the rest of the world, the SAF Cyber Defence Operations Hub was established "to defend MINDEF/SAF military networks against cyber threats."[8] In the light of these cyber threats, be it initiated by aggressive states actors or non-state enttities (like terrorists or rogue hacktivists), how should the SAF position itself in the evolving cyberspace?

This paper explores the offensive and defensive aspects of cyber warfare, and argues that the SAF should invest in cyber-defence rather than cyber-offence. By focusing on cyber-defence, the SAF not only deters potential military aggressions from state actors but also protects Singapore's civilian infrastructure and institutions from non-state entities.

CYBER WARFARE

The US Air Force describes cyber warfare as the ability 'to destroy, deny, degrade, disrupt, and deceive,' while at the same time 'defending' against the enemy's use of cyberspace for the very same purpose. The key instrument in conducting cyber warfare is the computer—it is a military weapon in the same way the sword, the battle tank, or the submarine is.[9] An article published in 2011,entitled *The New Cyber Arms Race,* depicts how cyber warfare might be conducted in the

Analysts and operators showing Minister for Defence, Dr Ng Eng Hen and then-Minister of State for Defence and Education, Mr Lawrence Wong (far right) how the C4 network and intelligence elements aid them during deployments.

future: *"Wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponised computer programmes that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement or troops, the path of jet fighters, the command and control of warships."*[10]

In fact, the future is already here. We have witnessed some forms of "weaponised computer programmes [aimed at] disrupt[ing] or destroy[ing] critical industries [and] disable[ing] military networks" in recent history. The employment of Stuxnet is one such example.[11]

CYBER-OFFENCE IN FOCUS: STUXNET

Described as the world's first cyber warfare weapon, Stuxnet was a complex malware designed to physically destroy a military facility.[12] Like any malware, Stuxnet infects a system through an external source like a USB flash drive. However, it only targets controllers from one specific manufacturer – Siemens. These controllers were used by Iran to run centrifuges that enrich nuclear fuel. Stuxnet compromised the logic controllers involved in the system and caused the centrifuges to spin out of control, damaging at least 14 industrial sites in the process, including a uranium-enrichment plant.[13] Due to the level of sophistication involved in the design and targeted execution of the malware against Iran, many observers believe that Stuxnet was created by a team of experts sanctioned by a national government. In other words, Stuxnet may well be a politically motivated cyber weapon used by a state actor against its adversary.[14]

A network-centric force is susceptible to disruptions to its command and control mechanism. The enemy can disable key components of a network-centric force, preventing commanders from issuing orders, units from communicating with one another, or even individual weapon systems from sharing essential information. It is the defence against such cyber-attacks that spurs network-centric militaries to establish teams of cyber experts.

While Stuxnet is an overt example of cyber-offence capabilities, Advanced Persistent Threat (APT) is a covert category of cyber-offensive works carried out by state actors against potential enemies.

ADVANCED PERSISTENT THREAT

APT involves continuous and stealthy hacking activities organised and carried out by governments against a specific target, such as another nation, in order to exploit vulnerabilities for political gains. The high degree of coordination involved in APT, along with its associated political motivation, differentiates it from regular hacking activities. Only state actors, with their resources and pool of expertise, can carry out the drawn-out and sophisticated works of APT as they patiently see the returns of these stealthy activities come to fruition.[15]

APT comprises several teams; each specialised to perform a particular task. First, a surveillance team studies and identifies the key vulnerabilities of the target. This preparation process can take months or years. Thereafter, having gathered enough information about the target, an intrusion team works to breach the system. Once the team has successfully intruded into the system, having gained access to sensitive information, an exfiltration team extracts the information the APT is intended for. Instead of extracting everything it can find, only specific files are retrieved in order to avoid suspicion. Often, victims of APT do not know that they have been targeted until it is too late. Moreover, there is little reliable evidence the victim can use to accuse

Wikipedia

Diagram depicting the life cycle staged approach of an Advanced Persistent Threat (APT) which repeats itself once complete.

the perpetrator.[16] Information gathered through APT can serve as critical intelligence for a military to conduct its onward operations. For instance, battle plans conceived by adversarial political and military leaders can be obtained, allowing pre-emptive actions to thwart possible interventions.[17]

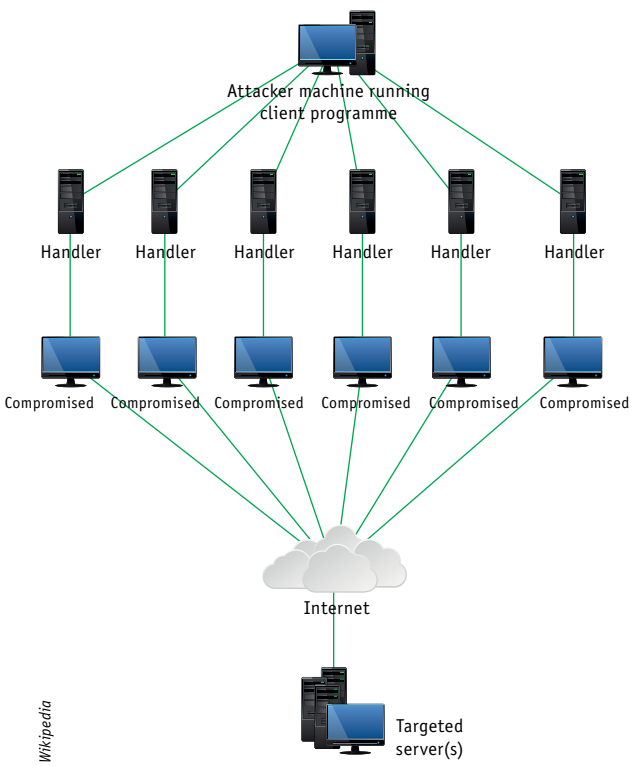
Given the effectiveness of Stuxnet as a cyber-weapon and the potential of APT to collect critical intelligence, investment and potential usage of cyber-offence capabilities may seem to be an obvious choice for the SAF if it wants to remain relevant in the evolving world of cyberspace. After all, obtaining these cyber-offence capabilities might deter potential adversaries of the SAF not just in cyberspace, but also in the conventional political space.

HOW A GOOD OFFENCE IS NOT THE BEST DEFENCE

In assessing the usefulness of cyber-offensive warfare to the SAF, it is important to note the core purpose of the SAF: "to enhance Singapore's peace and security through deterrence and diplomacy, and should these fail, to secure a swift and decisive victory over the aggressor."[18] Both overt cyber-offence (Stuxnet) and covert cyber-offence (APT) do not support the SAF's ability to ensure a swift and decisive victory. In addition, cyber-offence creates destabilising effects

in the political arena—the SAF will be better off focusing its resources elsewhere.

The development of sophisticated cyber weapons like Stuxnet requires a great deal of expertise and long periods of planning. Yet, the intended consequences, however carefully designed, are not always clear. There is difficulty in assessing the outcome of cyber-offence because the damage caused is not immediately apparent, unlike the use of conventional weapons. In the case of Stuxnet, recent research has suggested that the cyber weapon was ineffective and had caused negligible setback to Iran's nuclear programme—this is in direct contradiction to the widely-acclaimed success Stuxnet was thought to have achieved. Overall, the effects of Stuxnet were short-lived and Iran managed to overcome the cyber-attacks by 2010.[19] There might be unintended effects of cyber-offence as well. Besides Iran, Stuxnet infected over 60,000 computers from countries including China, United States, the United Kingdom and Australia.[20]



Distributed Denial-of-Service (DDoS) Stacheldraht attack diagram involved in the cyber-attack.

Regardless of the origin of Stuxnet, the uncontrollable spread of such cyber weapons might cause harm to the very nation it is meant to protect. Because cyber-offence involves uncertainty in delivering its intended payload, coupled with the long process it takes to materialise, it will not be able to ensure the swift and decisive victory desired by the SAF.

The stealthy nature of covert cyber-offence hinders trust between countries and hampers diplomacy. Even though cyber-attacks are meant to be stealthy, they are never absolutely undetectable because potential victims can follow the traces left behind by the cyber-attackers. When the *New York Times* suspected that its networks had been compromised, it worked with a computer security company and tracked down the cyber-attack. They found out that the attack was attributed to the Chinese military.[21] Revelations of such incidents have strained the diplomatic relationship between US and China. The US has blamed China for the theft of intellectual property and repeated attempts to gain a strategic advantage through cyber-attacks.[22] China has likewise made similar accusations against the US.[23] The political fallout resulting from cyber-offence continues to mar discussions between the two major powers, resulting in unintended destabilising effects to the international political arena at large. Cyber-offence carried out between US and China has invariably bred suspicions and hampered diplomatic efforts. As seen, both overt and covert forms of cyber-offence are counter-productive and undermine the SAF's role "to ensure peace and security through… diplomacy."[24] In the context of cyberspace then, a good offence is not the best defence; cyber-defence, not cyber-offence, is key.[25]

SINGAPORE'S VULNERABILITES AND IMPORTANCE OF CYBER-DEFENCE

The significance of cyber-defence for a nation that is heavily dependent on cyberspace cannot be overemphasised. Singapore, among the most wired countries in the world,[26] is dependent on cyberspace for many critical administrative processes like its e-government initiative.[27] Its increased connectivity

in cyberspace has resulted in an accompanying rise in vulnerabilities.[28]

Like Singapore, Estonia is also one of the world's most wired nations.[29] Most Estonians carry out administrative functions, such as banking transactions and paying taxes, online.[30] As such cyber warfare poses a real threat to its critical infrastructure and institutions. In 2007, Estonia experienced a massive cyberattack that threatened its national security. The cyber-attack involved distributed denial of service (DDoS) attacks that overwhelmed websites with a surge of requests that crippled the underlying network of servers. As a result, the functioning of government, banks, media and important institutions were brought to a halt.[31] Despite calls from Estonian officials for an international retaliation against the Russian government—whom they believe were the source of the attack—insufficient evidence existed to accuse Russia of staging these attacks.[32]

While Singapore has not seen cyber threats at the scale experienced by Estonia, it saw similar threats initiated by ill-intentioned individuals. In 2013, Singapore encountered a series of cyber-attacks initiated by the hacktivist organisation 'Anonymous'—a loose coalition comprising individuals who conduct hacking activities and defacement of websites, among other cursory works.

Singapore has much to learn from this incident. While the SAF Cyber Defence Operations Hub was established to defend the SAF's military networks against cyber threats, cyber-attacks need not necessarily target military installations to achieve a crippling effect to the nation's normal functioning. Cyber-attacks on critical civilian infrastructure can threaten national security just as in the case of Estonia. It is useful to note that cyber-offence in Estonia's case had no effect on protecting or repelling further cyber-attacks from its adversary; only cyber-defence could perhaps deny the adversary the ability to successfully intrude and cripple its computer networks. Effective cyber-defence could also block many additional cyber-attack attempts and weaken the will of adversaries, prompting them to stop trying. In comparing cyber-offence with cyber-defence, it is clear that the latter would be able to achieve a more tangible and stabilising effect—it could better protect critical infrastructure and ensure national security.

While Singapore has not seen cyber threats at the scale experienced by Estonia, it saw similar threats initiated by ill-intentioned individuals. In 2013, Singapore encountered a series of cyber-attacks initiated by the hacktivist organisation 'Anonymous'—a loose coalition comprising individuals who conduct hacking activities and defacement of websites, among other cursory works. The perpetrator, who went by the alias 'The Messiah,' temporarily disabled up to nineteen government websites.[33] Although the impact of these cyber-attacks was nothing more than fear mongering, the incident underlined the inherent vulnerability Singapore faces given its heavy dependence on cyberspace. Despite the SAF's focus on cyber-defence exclusively aimed at protecting military installations and infrastructure, the processes and organisations developed in enhancing its cyber security can be transferred to civilian operations. Singapore as a whole can then benefit as a result of the SAF's strengthening of cyber-defence capabilities on non-military infrastructure.

BOOSTING CYBER-DEFENCE

In order to create a robust cyber-defence structure, defenders can target three main points of entry cyber-attackers typically exploit: Confidentiality, Integrity, and Availability—collectively known as the CIA triad. Confidentiality means that no information is revealed to unauthorised personnel—only individuals with the rights and privileges are given access to such

information. Integrity refers to the intactness of information as it is transmitted and then received —data integrity assures that information is not compromised. Availability means that resources and access to information are unimpeded.[34] In the case of the cyber-attacks by 'Anonymous' on the Singapore government in 2013, which involved the defacement and temporary shutdown of websites, integrity and availability were compromised.

That said, the country's robust cyber-defence structure was able to recover quickly and websites were back up and running within hours following the attacks, partially due to the low calibre and uncoordinated nature of the attack by 'Anonymous'. Such is a demonstration of another hallmark of good cyber-defence—resilience. A resilient cyber-defence structure has the capacity to work under degraded conditions and if compromised, is able to recover quickly. Also referred to as intrusion-tolerant,'[35] a resilient cyber-defence structure is only as strong as the human component undergirding it.

In terms of system measures, careful issuance and monitoring of access control ensure that the overall cyber-defence structure prevents not only external threats but internal ones as well. It is crucial to acknowledge that sometimes the danger comes from the inside.

In 2008, the US military suffered an unprecedented compromise of its classified military computer networks because an unauthorised flash drive carrying a malware was carelessly inserted into an official computer in the Middle East.[36] The damage done encompassed confidentiality and integrity —the enemy who implanted the malware knew classified information about the US military and communication lines within the US military no longer ensured data integrity. All these because one soldier made the mistake of not scanning the flash drive for malware before inserting it into the computer.[37]

Ensuring the compliance of personnel regarding cyber-defence matters is critical in maintaining the robustness of safeguards already put in place. The SAF employs cryptographic integrity checks to ensure the secure communication of classified information. These work in tandem with personnel's efforts to maintain information security. This includes refraining from introducing unauthorised external devices to internal computer networks.

In terms of system measures, careful issuance and monitoring of access control ensure that the overall cyber-defence structure prevents not only external threats but internal ones as well. It is crucial to acknowledge that sometimes the danger comes from the inside. The sensational leaks of classified information in cases like Edward Snowden and Bradley Manning show that failure in access control can result in a devastating compromise of the entire cybersecurity architecture.[38] Edward Snowden, a low-level defence contractor working for the CIA, was given high-level access to classified documents which he would later leak to the press. Access control was too lax and provided the loopholes which whistleblowers like Snowden exploited. The sheer amount of information that he was able to sneak out of supposedly highly-secure computer systems is unfathomable. Learning from these incidents, the SAF should constantly review its access control processes and ensure shortcomings are rectified. Only then can the possibility of leakages be minimised, and confidentiality of information maintained. On top of looking outward for external cyber-attacks, a robust cyber-defence structure must look inward to prevent internal sabotage.

CONCLUSION

The SAF has entered a new era of warfare where cyberspace plays an integral role in military operations and national security. The discovery of cyber weapons like Stuxnet, the reality of APT and the unfolding of international crises like the cyber-attacks on Estonia, all point to the need for the SAF to continually adapt and evolve itself to cope with cyber threats. With the establishment of the SAF Cyber Defence Operations Hub

which focuses on strategies, tactics and doctrines to cope with cyber warfare, the SAF needs to assess the current development and capabilities of both cyber-offence and cyber-defence and decide how much of each it should focus on. Through the analysis of the offensive and defensive aspects of cyber warfare, this paper has shown that the SAF should invest in cyber-defence rather than cyber-offence. By putting emphasis on cyber-defence, the SAF not only deters potential military aggressions from state actors but also protects Singapore's civilian infrastructure and institutions from non-state entities.

ENDNOTES

1. Arthur K. Cebrowski and John J. Garstka. "Network-centric warfare: Its origin and future." *US Naval Institute Proceedings* 124, n._1 (1998), 28-35.
2. MINDEF (Singapore). "3rd Generation SAF." http://www.mindef.gov.sg/imindef/key_topics/3rd_generation_saf.html

   Claire Apthorp. "Singapore Leads The Way." *Defence Review Asia* 4, issue 6 (2010): 22.
3. Michael Dillon, "Network society, network-centric warfare and the state of emergency." *Theory, Culture & Society* 19, n._4 (2002), 71-79.
4. US Department of Defense Joint Publication 1-02. *Dictionary of Military and Associated Terms:* 141.
5. US Army Cyber Command. "Organization." http://www.arcyber.army.mil/org-uscc.html

   Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute. https://project2049.net/publications.html
6. Mazanec, M. Brian. "The art of (cyber) war." *Journal of International Security Affairs* 16 (2009), 84.
7. Ministry of Foreign Affairs (Singapore). "Foreign Policy." http://www.mfa.gov.sg/content/mfa/overseasmission/manila/about_singapore/foreign_policy.html
8. MINDEF (Singapore). "Clarification of the role of the SAF Cyber Defence Operations Hub (CDOH)." http://www.mindef.gov.sg/imindef/press_room/clarification/11Nov13_clarification.html#.UzA7s61dW9o
9. Peter W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* (Oxford: Oxford University Press, 2013), 128.
10. Mark Clayton. "The New Cyber Arms Race." *The Christian Science Monitor.* http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.
11. David Kushner. "The real story of Stuxnet." *Spectrum, IEEE 50,* n._3 (2013), 48-53.
12. Ralph Langner. "Stuxnet: Dissecting a cyberwarfare weapon." *Security & Privacy, IEEE 9,* n._ 3 (2011), 49-51.
13. David Kushner. "The real story of Stuxnet." *Spectrum, IEEE 50,* n._3 (2013), 48-53.
14. Sascha Knoepfel. "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War." *Cyberspace and International Relations.* Springer Berlin Heidelberg, 2014, 117-124.
15. Colin Tankard. "Advanced Persistent threats and how to monitor and deter them." *Network Security,* n._8 (2011), 16-19.
16. Peter W. Singer, and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2013), 56-60.
17. Adam Taylor. "By banning YouTube, has Turkey revealed just how damning today's leaked recording is?" *Washington Post.* http://www.washingtonpost.com/blogs/worldviews/wp/2014/03/27/by-banning-youtube-has-turkey-revealed-just-how-damning-todays-leaked-recording-is/
18. MINDEF (Singapore). "Mission." http://www.mindef.gov.sg/imindef/about_us/mission.html
19. Ivanka Barzashka. "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme." *The RUSI Journal* 158, n._2 (2013), 48-56.
20. James P. Farwell and Rafal Rohozinski. "Stuxnet and the future of cyber war." *Survival* 53, n._1 (2011), 23-40.
21. David E. Sanger, David Barboza and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times*

    http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all

22. Sanger, David E. "U.S. Blames China's Military Directly for Cyberattacks." *New York Times*. http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0

23. Jacob Davidson. "China Accuses U.S. of Hypocrisy on Cyberattacks." *Time*. http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/

24. MINDEF (Singapore). "Mission." http://www.mindef.gov.sg/imindef/about_us/mission.html

25. Peter W. Singer, and Allan Friedman. "Cult of the Cyber Offensive: Why belief in first-strike advantage is as misguided today as it was in 1914." *Foreign Policy,* January 15, 2014. http://www.foreignpolicy.com/articles/2014/01/15/cult_of_the_cyber_offensive_first_strike_advantage

26. Bloomberg. "Most Wired in the World: Countries." http://www.bloomberg.com/visual-data/best-and-worst/most-wired-in-the-world-countries

27. Singapore Government. "About eGov: Introduction." http://www.egov.gov.sg/about-egov-introduction

28. Beidleman, W. Scott. "Defining and Deterring Cyber War." *U.S. Army War College Carlisle Barracks* PA, 2009.

29. Jacob Davidson. "China Accuses U.S. of Hypocrisy on Cyberattacks." *Time,* July 1, 2013. http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/

30. Christopher Rhoads. "Politics & Economics: Estonia Gauges Best Response to Cyber Attack." *The Wall Street Journal,* 2007.

31. Joshua Davis. "Hackers Take Down the Most Wired Country in Europe." *Wired Magazine,* issue. 15.09 (2007).

32. Michael Lesk. "The new front line: Estonia under cyberassault." *IEEE Security & Privacy* 5, n._4 (2007): 76-79.

33. F.C. "Hacking in Singapore: Messiah complicated." *The Economist*. http://www.economist.com/blogs/banyan/2013/12/hacking-singapore

34. Baumann, Rainer, Stéphane Cavin, and Stefan Schmid. "Voice over IP-security and SPIT." *Swiss Army, FU Br* 41 (2006), 1-34.

35. Yves Deswarte, Laurent Blain, and J-C. Fabre. "Intrusion tolerance in distributed computing systems." *IEEE Symposium on Security and Privacy,* Oakland, California (1991), 110-121.

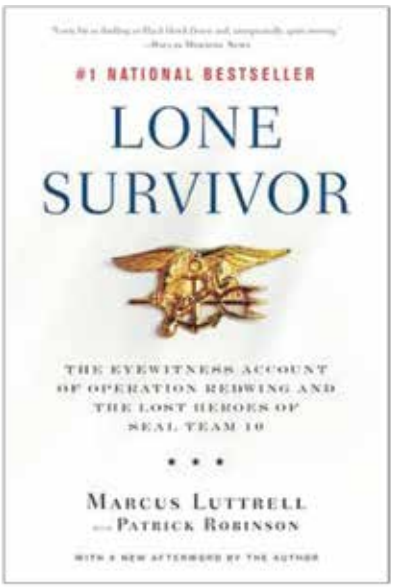
36. Lynn, J.William. "Defending a new domain: The Pentagon's cyberstrategy." F*oreign Affairs* (2010), 97-108.

37. P.W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2013). 64.

38. Glenn Greenwald, Ewen MacAskill, and Laura Poitras. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." *The Guardian* 9 (2013).

LTA Ng Yeow Choon is a Fighter Pilot by vocation. He was awarded the SAF Merit Scholarship in 2012 and is currently pursuing his Bachelors of Arts in Economics at New York University. LTA Ng received a Commendation Award at the Chief of Defence Force Essay Competition 2013/2014.

Book Review



Marcus Luttrell & Patrick Robinson, Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10, (New York: Little, Brown and Company), 2008, 464 pages

By **Joshua Foo**

INTRODUCTION

Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10 by Marcus Luttrell tells the harrowing story of a soldier and his elite team out on a mission in Afghanistan. In this gripping non-fiction, four United States (US) Navy SEALs (Sea Air & Land) embarked on a reconnaissance mission in the mountainous terrain of the Afghan-Pakistan border. They had only one objective—to gather essential information on an Al Qaeda member believed to be close to Osama Bin Laden in a Taliban-controlled zone. Sadly, only one SEAL survived.

Born and raised in Texas, Marcus Luttrell was drilled into facing the harsh realities of life with his twin brother since a tender age. His father always dreamt of them being Navy SEALs. Prior to his enlistment into the Navy, he trained under a retired Green Beret sergeant, Billy Shelton. Following months of determined training and countless tests, he survived the Basic Underwater Demolition/ SEAL (BUD/S) training and finally earned the coveted SEAL trident. After recovering from injuries and successfully graduating from BUD/S Class of 228, Luttrell continued his training as a Special Operations Combat Medic. He was then deployed to Afghanistan in 2005, when the tragedy happened. Luttrell was discharged from the Navy, having served with the elite SEALs, survived one of the deadliest battles in Afghanistan and earned a Navy Cross for extraordinary heroism in combat.[1]

TARGETED AUDIENCE

Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10 is targeted at those seeking a true story that showcases American heroism, Afghan humanity and threat-to-terrorise all in one. This thrilling book which is insightful and revealing, promises to be an exciting read.

THE BUILD UP

Luttrell described his experinces from the rigours of SEAL training, where he and his fellow SEALs discovered what it took to join the most elite of America's famed special forces, to a fight in the desolate hills of Afghanistan for which they could never have been prepared. His first-person account of his comrades' heroism shows an experience that is both terrifying and uplifting at the same time. In this uncompromising tale of unflinching courage and noble sacrifice, honour and unabashed patriotism, Marcus Luttrell delivers a powerful story of modern war.

The story unfolds as his elite unit infiltrates into enemy territory. The mission is foreseen to be tough due to the mountainous terrain, lack of intelligence and potentially overwhelming numbers of Taliban fighters. With their advanced training, they were sent to one of the most problematic regions of Afghanistan to stop the Taliban from inflicting further terror attacks.

SEAL fire team leader Marcus Luttrell led Operation Red Wings, the extraordinary exchange of fire that led to the largest loss of life in the US Navy SEAL history. As the only one still alive to tell the story, he constantly commends his team mates who fought valiantly beside him throughout the battle. Over the next four days, as the bulk of the story unfolds, he describes how a Rocket-Propelled Grenade (RPG) blasted him into an area where the enemy forces could not locate him. Terribly injured, he was presumed to be dead. He endured his grave injuries and thirst and crawled for miles through the mountains.[2]

The SEALs fought long and hard, with Luttrell illustrating their determination and grit, but the four soldiers on the ground were fighting nearly 100 Taliban fighters with no backup. Losing their equipment and being massively outnumbered, three of the four-man team lost their lives. As a last-ditch effort for survival, one used a satellite phone that betrayed their location. A rescue team quickly responded but was shot down, causing even more lives to be lost.[3]

As this true and deeply saddening story unfolds, readers will find themselves more and more deeply immersed and grimacing for the loss of the many elite soldiers who died.

THE SURVIVAL

Luttrell credits his survival to sympathetic villagers who risked their lives to take him in and keep him safe from Taliban insurgents. With Luttrell injured and alone in enemy territory struggling for survival, Afghan villagers found him and decided to protect him at all costs. Together, they plotted to evade the Taliban and to make known to the US military his whereabouts. Meanwhile, Luttrell's family back in Texas already knew he was missing in action, with friends and comrades all praying for his survival.[4] He had close encounters where Taliban used the knowledge of the local terrain to their advantage to hunt him down. However, the villagers refused to accede to the Talibans' requests and continued to protect him. When the much awaited rescue finally came, he was given the best medical attention and commended by many of his senior commanders.

Luttrell was the only one of four men to survive after a running battle with dozens of Taliban rebels. Eight members of the Navy SEALs and eight Army Special Operations Aviators who came by helicopter to rescue the original team were shot down, and all were killed. The book, revolving around his survival, both in training and during the battle, was also filled with unabashed patriotism and blamed the 'liberal media' for its role in sustaining military Rules of Engagement (ROE) that prevent soldiers from killing unarmed civilians, who may also be scouts or informers for hostiles.[5]

OPERATION RED WINGS

On the night of 27th June 2005, two MH-47 Special Operations Aircraft of the Army Special Operations Command's 160th Special Operations Aviation Regiment (SOAR) approached Sawtalo Sar, Afghanistan. Luttrell describes the clear night as one of the helicopters performed decoy landings to confuse the enemy on the ground,

while the other inserted Luttrell and his team. The four-man SEAL team landed via fastrope between Sawtalo Sar and Gatigal Sar. The team included team leader Navy Lieutenant Michael P. Murphy of SEAL Delivery Vehicle Team 1; Petty Officer Second Class Danny P. Dietz from SEAL Delivery Vehicle Team 2; Petty Officer Second Class Matthew G. Axelson; and Luttrell himself. After moving to a pre-planned position where they could perform their surveillance, the team was discovered by local goat herds. After determining that they were civilians and thus not combatants, Lieutenant Murphy had them released, according to the ROE which Luttrell persistently criticises.

Operation Red Wings was a joint military operation during the War in Afghanistan in the Pech District of Afghanistan's Kunar Province, on the slopes of Sawtalo Sar. Operation Red Wings intended to disrupt local anti-Coalition Militia activity, thus contributing to regional stability and helping to facilitate the Afghan Parliament elections which were scheduled for September 2005.[6] At the time, anti-Coalition Militia activity in the region was carried out most notably by a small group led by Ahmad Shah, a local man from Nangarhar Province, His small group were among the primary targets of the operation.

Upon Luttrell and his team realising that letting the goat herds go would compromise their positions, they retreated to a fallback position. Within the next hour, Shah and his men ambushed the SEAL team in the dark, over the slopes of Sawtalo Sar. They were heavily armed with RPK light machine guns, AK-47s, RPG-7 RPG, and 82mm mortars.[7] The SEAL team was forced into the north-eastern gulch of the slopes due to the intense amount of fire they were bombarded with. Unable to contact their operations headquarters, the SEALs were unable to request for back up until a satellite phone was used. Three of the four team members were killed, and the only survivor, Marcus Luttrell, was left seriously injured with a number of fractures He was subsequently rescued by local Pashtuns who ultimately saved his life, for in his current condition and without assistance, he would surely have been killed or captured by the Taliban.

DIFFERENT LEVELS

Lone Survivor's first layer is the surface plot: a Navy SEAL, after completing his torturous training, is sent to Afghanistan and then further deployed on a special operation to comb the mountains for an extremely dangerous Taliban leader. The closely-knit team of four were ambushed early in the mission, with three of them brutally killed in front of the author's eyes.[8] This was painful, gripping and kept readers on the edge of their seats.

On the next level, Luttrell believes that the only reasons why he survived the ordeal were the superiority of the SEALs in terms of their physical skills, determination and his belief in God.

Exploring further, a deeper understanding in this book is the mention of politics. According to Luttrell, his team died in vain as a result of the liberal media and decision-makers in the government imposing restrictions and limitations with the ROE. This layer is filled with hatred and denunciation, understandably, in the defence of his fallen comrades. A good example is when they chose to set the harmless-looking goat herders free when they were conducting their reconnaissance early in the mission. Multiple references were made in the later parts of the book on this decision as it appeared that that the goat herders revealed their whereabouts and this led to their deaths. The decision to release the goat herders was in accordance to the ROE. Luttrell put it bluntly, "I can say from first hand experience that those Rules of Engagement cost the lives of three of the finest US Navy SEALs who have ever lived."[9] An unintended irony was achieved when a Pashtun villager from a neutral tribe in the mountains of Afghanistan, saved his life.[10] Luttrell would have shot the villagers (who protected him and saved his life) had he had the strength to. Not shooting civilians (the goat herders) may have caused

his team to land in an ambush, but not doing so also kept him alive.

Finally, there is the deepest and darkest layer, the last level of melancholy that looms over *Lone Survivor*. At times, the book reads as a psychological thriller, one that would end with, "I woke up drenched in cold sweat, palms clammy and heart racing. It was just a terrible nightmare."[11] Luttrell appears to be haunted by nightmares after he witnesses the horrific battlefield deaths of his three fellow SEALs, with him saying, "Again in my mind I heard that terrible, terrible scream, the same one that awakens me, bullying its way into my solitary dreams night after night, the confirmation of guilt."[12] Nobody but he knows exactly what happened during the Operation. No recordings and photos were taken. The story could have been fictitious and dramatized to a certain extent. Operation Red Wing's disaster began with the decision to let the goat herders go, due to the practice of ROE. The death of his fellow SEALs was blamed on the liberals, politicians and the media. This book is a story about Marcus Luttrell, torn by the deaths of his best friends and fellow SEALs, facing the inability to accept the loss. Indirectly, he blames liberal media, politicians, Al Qaeda and Islam.

That said, Luttrell and his comrades were Navy SEALS and were very proud of being one. They were extraordinary soldiers; their training was more demanding, and they were often sent to the toughest areas of the world to fight in the name of global peace. The book was both gripping and extremely dark for readers. *Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10* gives us an insight into what the best soldiers put themselves up against. It also tells us exactly how dark some parts of the world still are.

ENDNOTES

1, M. Luttrell, P. Robinson, *Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10* (New York: Little, Brown and Company, 2007),

2. Ibid., 101.

3. Ibid., 97.

4. Ibid., 187.

5. Ibid., 127.

6. E. Darack, *Victory Point: Operations Red Wings and Whalers – The Marine Corps' Battle for Freedom in Afghanistan* (New York, Penguin Group, 2010).

7. M. Luttrell, P. Robinson, *Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10* (New York: Little, Brown and Company, 2007), 199.

8 Ibid., 210.

9. Ibid., 255.

10. Ibid., 236.

11. Ibid., 268.

12. Ibid., 269.

Winston Churchill (1874-1965)

by **Tan Wallace**

INTRODUCTION

Winston Churchill was a brilliant orator, an eloquent writer, an earnest artist and a charismatic politician. He is best known for leading a successful Allied strategy to defeat the Axis powers during World War Two (WWII).

EARLY LIFE

The Right Honourable Sir Winston Leonard Spencer Churchill was born to a privileged aristocratic family on 30th November, 1874. Since both his parents were frequently travelling and away from home,[1] Churchill was taken care of mainly by his nanny, Elizabeth Everest, whom Churchill fondly called 'Woomany.'[2]

Just before his eighth birthday in 1882, Churchill enrolled into an elite preparatory school, St George's at Ascot. Though he was never an outstanding student, he was well-liked by his peers. In 1887, at the age of twelve, Churchill went to Harrow, a reputable school situated near London, where he began studying military tactics. In 1893, upon graduation, Churchill enrolled into the Sandhurst Royal Military College. Churchill's distant relationship with his parents was made evident as his parents seldom visited him while he was in school, despite his pleas. In December 1894, Churchill graduated as one of Sandhurst's top students and was commissioned as a cavalry officer thereafter.[3]

WAR CORRESPONDENT

Upon completion of his basic military training, Churchill travelled to Cuba while on his leave to witness the rebellion being put down by the Spanish forces. In 1895, after his leave was over, he joined the 4th (Queen's Own) Hussars to serve in India and Sudan, where he joined the Battle of Omdurman in 1898. During this period, he developed an interest in writing. He also started supplying military reports for the Daily Telegraph and published *The Story of the Malakand Field Force* (1898) and *The River War* (1899).[5] After leaving the British Army in 1899, Churchill started working for the *Morning Post* as a war correspondent. Unfortunately, he was captured by the Boers during his coverage on the Boer War in South Africa but made headlines after managing to escape captivity within a month. Upon his return to England, he wrote about his experiences while being captured in the book, *London to Ladysmith* (1900).

Location of the Battle of Omdurman.[6]

ROAD TO POLITICS

In 1900, the 25 year-old Churchill ran for election for the first time with the Conservative Party and was voted in as the Member of Parliament (MP) for Oldham, Manchester. Few would have expected that this was the start of the successful political career of Britain's future prime minister.

It was not long before Churchill became widely known for his brilliant speeches made during parliamentary sessions in support of social change to help the poor and less fortunate. In 1904, Churchill decided to switch to the Liberal Party after it became clear that he did not hold the beliefs of the Conservatives.[7] He went on to win the 1906 General Election under the newly formed Liberal government, holding the appointment of the Under-Secretary of State for the Colonies. Having a reputation for strong dedication, Churchill was appointed President of the Board of Trade in the Prime Minister's Cabinet in 1908. In the same year, he married his fiancée, Clementine Ogilvy Hozier. As the President of the Board of Trade, Churchill continued to help the poor by introducing Britain's first ever minimum wage, setting up labour exchanges for the unemployed, and at the same time, implementing national unemployment insurance to provide aid to those who are unable to find a job during that time. Churchill also expedited the approval of the People's Budget, which introduced new forms of taxes on the rich which will be channelled to the funding of new social welfare programmes.

Winston Churchill subsequently became the First Lord of the Admiralty in October 1911 and started modernising the British Navy, demanding that newly constructed warships be switched from coal-fired to oil-fired engines as the latter were more energy efficient and produced less smoke so that the fleet would not reveal its presence easily.[8] For the next three years, Churchill continued to improve the British Navy while keeping a watchful eye on Germany's growing military prowess. Foreseeing the great military potential of aeronautical technology, he established the Royal Naval Air Service to fully utilise it.[9]

Churchill joined the War Council when war broke out in 1914. Although he was not involved in the Battle of Gallipoli, he was ultimately blamed for the failure of the entire campaign and was subsequently forced out of politics.[11] He then re-joined the British Army, commanding the 6th Battalion, Royal Scots Fusiliers (an infantry regiment) on the Western

Front for almost two years. Soon after David Lloyd George took over from Herbert Asquith as the Prime Minister, Churchill was appointed Minister of Munitions, primarily overseeing the production process of tanks, aeroplanes, guns and shells for the rest of the war. Churchill then briefly assumed the role of Secretary of State for the Colonies before losing his MP seat a year later due to fractures and divisions within the Liberal Party. This prompted him to re-join the Conservatives where he held the title of Chancellor of the Exchequer until the Conservative government was defeated in 1929. And for the second time, Churchill was out of the government. However, he managed to retain his role of MP this time round. This gave him more time to focus on his writing, which included the publication of the *History of the English Speaking Peoples*. His seat in parliament ensured that he still had a say in world affairs, mostly warning the government of Germany's growing threat.

WORLD WAR II

Churchill quickly became a leading advocate for British rearmament after Adolph Hitler rose to power in 1933. Though he disliked the communist founded Soviet Union, he firmly maintained that Britain and France should form an alliance with the communist state and was especially critical of then British Prime Minister Neville Chamberlain's policy of appeasement towards Nazi Germany.[12] Churchill believed that appeasement will be futile because of Hitler's irrational aims and objectives. As such, no amount of appeasement would satisfy him—he would always want more. On 3rd September, 1939, after nearly ten years out of the government, Churchill was appointed First Lord of the Admiralty for the second time as war was imminent. He went on to become the Chairman of the Military Coordinating Committee on 4th April, 1940.

After Germany invaded Norway, which was previously deemed by Chamberlain to be a vital stronghold for Britain to deter any potential aggression by Germany, parliament passed a vote of no confidence against Chamberlain. Britain was without a prime minister, with the possibility of war looming in the background. This prompted King George VI to quickly appoint Churchill as the new Prime Minister. Just a day after Germany successfully invaded the Netherlands, Belgium, Luxembourg, and France, Churchill delivered his 'Blood, Toil, Tears, and Sweat' speech in the House of Commons in a bid to galvanise the British to fight against the seemingly unbeatable Germany. Churchill wasted no time in forming a coalition government with leaders from the Labour, Liberal and Conservative parties, utilising the best talent Britain had, regardless of their political stance. Knowing that the British stood no chance against Germany without the help of the United States (US), the ever pragmatic Churchill swiftly formed an alliance with the US, which was made easier because of his good relationship with then US President, Franklin D. Roosevelt. By March 1941, Britain was able to obtain essential aid from the US via the 'Lend Lease Act,' which allowed Britain to order war supplies from the US on loan.[13]

Churchill was more confident than ever that the Allies will go on to win the war against the Axis Powers after the US entered

Winston Churchill with the Naval Wing of the Royal Flying Corps.[10]

the war to fight against Germany in December 1941. Churchill collaborated with US President Roosevelt and Soviet Union leader, Joseph Stalin in the subsequent months that followed, to devise a war strategy for the Allies that would eventually lead to the success of the war against Germany.

Despite receiving much credit for the victory of the war, it did not prevent Churchill from losing the 1945 General Elections to the Labour Party, forcing him to resign. Many British had felt that Churchill had lost touch with daily life after years of war. For the following six years, Churchill continued to have an influence on British politics as the Leader of the Opposition. In March 1946, while visiting US, he delivered his famous 'Iron Curtain' speech, warning them of Soviet ascendancy in Eastern Europe. He also stood firm in his belief that Britain should remain independent from Europe.[14] It was during this period of time that he was able to pursue his hobbies such as writing and painting.

SECOND TERM

After the 1951 General Elections, Churchill was made Prime Minister for the second time. He continued helping the poor through the 'Mines and Quarries Act' of 1954 which ensured the safety and well-being of the miners and raised the standard of housing by implementing the 'Housing Repairs and Rent Act' of 1955 which largely benefited tenants.

RETIREMENT AND DEATH

However, age was catching up with Churchill. His health deteriorated gradually after suffering multiple strokes while working in his office at 10 Downing Street. This news was not made known to the public. Instead, they were told that Churchill suffered from exhaustion. It soon became clear that Churchill's physical and mental state meant that he could no longer continue as Prime Minister for much longer. On 5th April, 1955, the 80 year-old Churchill reluctantly resigned, due to failing health. However, he remained as a MP until 1964 when he did not participate in the re-election due to poor health. On 15th January, 1965, Churchill suffered a severe stroke that left him in a coma. On 24th January, 1965, he died at the age of 90 in his London home at Hyde Park Gate with his wife Lady Clementine Churchill and other members of the family at his bedside. Churchill was given a state funeral by the decree of Queen Elizabeth II at St Paul's Cathedral after his body was laid in the Palace of Westminster where close to 300,000 people came to pay their last respects.

LEGACY

Churchill is undoubtedly one of the greatest leaders of the 20th century. Nicknamed the 'British Bulldog', he thrived in adversity. In his first speech as Prime Minister, Churchill told the House of Commons that "I have nothing to offer but blood, toil, tears and sweat." His unbounded optimism during Britian's darkest hour ensured that the British citizens upheld their belief of winning the war. This was seen by his trademark 'V for Victory' sign whenever he was seen in public.

He also demonstrated that communication was a vital skill through his inspirational speeches that were delivered in a simple but precise manner, allowing him to forge a common identity with the people of Britain, thus enabling him to achieve important goals for the country and ultimately, winning the war against Germany.

His great foresight in pioneering the aeronautical technology also led to the superiority of the Royal Naval Air Service over their German counterparts.

Churchill proved to be a pragmatic leader, placing objectives above all. This was evident when he formed an alliance with the communist governed Soviet Union despite his strong dislike and disapproval of communist ideology. After being appointed the Prime Minister by King George VI, instead of choosing politicians from his own party to assume senior appointments for the war, Churchill decided to pick the best politicians from the different political parties, casting aside their political indifferences and prioritising the nation's survival.

Till today, Churchill is still remembered as the man who led Britain's defence against Hitler's invasion.

ENDNOTES

1. National Churchill Museum, "Winston's Parents," http://www.nationalchurchillmuseum.org/winston-churchills-parents.html
2. National Churchill Museum, "Winston's Nanny," https://www.nationalchurchillmuseum.org/winston-churchill-nanny.html
3. Jennifer Rosenberg, "Sir Winston Churchill," http://history1900s.about.com/od/people/a/Churchill.htm
4. Abroad In The Yard, "Winston Churchill sees Irish VC winner in action at Battle of Omdurman 1898, and becomes skin graft donor," http://www.abroadintheyard.com/winston-churchill-sees-irish-vc-winner-in-action-battle-of-omdurman-and-becomes-skin-graft-donor/
5. Jennifer Rosenberg, "Sir Winston Churchill," http://history1900s.about.com/od/people/a/Churchill.htm
6. University of Texas Libraries, "Perry-Castañeda LibraryMap Collection"http://www.lib.utexas.edu/maps/cia01/sudan_sm01.jpg
7. Ben Draper and Jak Brown, "Sir Winston Churchill" https://www.gov.uk/government/history/past-prime-ministers/winston-churchill
8. Erik J. Dahl, "From coal to oil," www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA524799
9. John Simkin, "Royal Naval Air Service," http://spartacus-educational.com/FWWrnas.htm
10. Wikipedia, "Winston Churchill With Naval Wing of the Royal Flying Corps," http://upload.wikimedia.org/wikipedia/commons/d/d0/Winston_Churchill_With_Naval_Wing_of_the_Royal_Flying_Corps,_1914._CH4778.jpg
11. National Churchill Museum, "World War I and its Aftermath," http://www.nationalchurchillmuseum.org/churchill-in-world-war-i-and-aftermath.html
12. Andy Newman, "Sir Winston Churchill and the Anti-fascist War," http://socialistunity.com/sie-winston-churchill-and-the-anti-fascist-war/
13. John Simkin, "Lend-Lease," http://spartacus-educational.com/2WWlendlease.htm
14. Biography, "Winston Churchill," http://www.biography.com/people/winston-churchill-9248164

Quotable Quotes

I think whether you're having setbacks or not,
the role of a leader is to always display a winning attitude.
– Colin Powell (b. 1937), American statesman,
retired Four-star General in the United States Army.

Our attitude towards others determines their attitude towards us.
– Earl Nightingale (1921-1989), motivational speaker, author.

Publicity is a great purifier because it sets in actions the forces of public opinion,
and in this country public opinion controls the courses of the nation.
– Charles Evans Hughes (1862-1948), politician, lawyer, professor, judge.

The eyes see not what is before them when the mind is intent on other matters.
– Publilius Syrus (fl. 46 BC-29 BC), writer.

He who learns but does not think, is lost! He who thinks but does not learn is in great danger.
– Confucius (551–479 BC), teacher, editor, politician, philosopher.

It's fine to celebrate success but it is more important to heed the lessons of failure.
– Bill Gates (b. 1955), American business magnate,
philanthropist, investor, computer programmer, inventor.

Far better is it to dare mighty things, to win glorious triumphs,
even though checkered by failure... than to rank with those poor spirits who
neither enjoy nor suffer much, because they live in a grey twilight that knows not victory nor defeat..
– Theodore Roosevelt (1858-1919), 26th President of the United States.

Sometimes by losing a battle you find a new way to win the war.
– Donald Trump (b. 1946), businessman, investor, television personality, author.

A failure is not always a mistake; it may simply be the best one can do under the circumstances. The real mistake is to stop trying.
– Burrhus Frederic Skinner (1904-1990), psychologist, behaviourist, author, inventor, social philosopher.

My great concern is not whether you have failed, but whether you are content with your failure.
– Abraham Lincoln (1809-1865), 16th President of the United States.

A positive attitude causes a chain reaction of positive thoughts, events and outcomes. It is a catalyst and it sparks extraordinary results.
– Wade Boggs (b. 1958), professional baseball third baseman.

Someone is sitting in the shade today because someone planted a tree a long time ago.
– Warren Buffett (b. 1930), business magnate, investor, philanthropist.

Do the things you know and you shall learn the truth you need to know.
– Louisa May Alcott (1832-1888), novelist.

If opportunity doesn't knock, build a door.
– Milton Berle (1908-2002), comedian, actor.

Man never made any material as resilient as the human spirit.
– Bernard Williams (1929-2003), moral philosopher.

Ideas shape the course of history.
– John Maynard Keynes (1883-1946), economist.

What great thing would you attempt if you knew you could not fail?
– Robert H. Schuller (b. 1926), televangelist, pastor, motivational speaker, author.

When your values are clear to you, making decisions becomes easier.
– Roy E. Disney (1930-2009), Vice Chairman, The Walt Disney Company.

Be the chief but never the lord.
– Lao Tzu (604-531 BC), philosopher, poet.

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, preferably in OpenOffice 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 licence 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

Features

ISSN 2017-3956