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