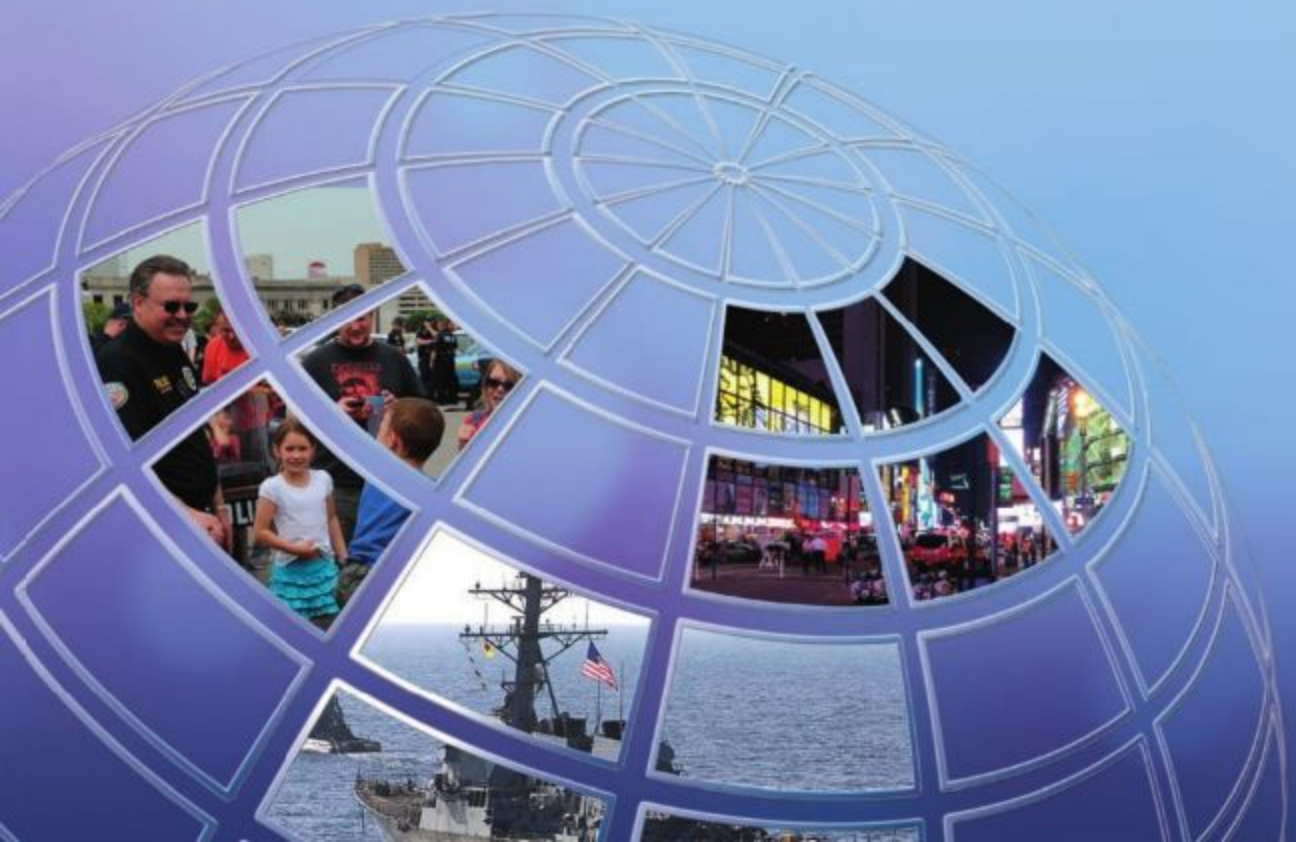
POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

Vol. 44 No. 4 [2018]



Editorial Board

ISSN 2017-3956 Vol. 44 No. 4 [2018]

contents

contents

Editorial

We mark the end of 2018 with our final issue of the year, Pointer Vol. 44, No. 4. As we wind down and celebrate the festivities with our loved ones, we bear in mind the varied events that have happened, both globally and locally and the impact they have on us—whether it is the security threat from the ever-present terrorist danger that menaces us, to the increasingly sinister attacks in the cyber domain and false news, to trade wars that all have serious impact on Singapore as a whole. To be sure, it is crucial that Singaporeans unite to deal with these threats together. As Minister for Defence, Dr Ng Eng Hen puts it: "To respond to these ever-evolving threats, we need a collective will, a Total Defence to stand as one people united in resolve and action."[1]

The essays in this issue cover a diverse list of topics with novel ideas like crowdsourcing intelligence to prevent lone-wolf attacks on Singapore's Smart Nation efforts. We have also included other subjects like hybrid warfare, social media in the military, the dangers of unmanned aerial vehicles as well as the various challenges facing the Singapore Armed Forces (SAF) as it moves steadfastly beyond the past five decades of its development.

The essay entitled, 'Crowding Out the Lone-Wolf – Crowdsourcing Intelligence to Prevent Lone-Wolf Attacks' is by MAJ Jeffrey Ng Zhao Hong. According to MAJ Ng, with terrorist networks turning toward lone-wolf attacks as their choice modus operandi, homeland security forces are quickly realising that traditional top-down surveillance programmes are ill-suited to detect the subtle indicators of sporadic attacks perpetrated by legal residents with no known links with terrorist cells. In this essay, MAJ Ng studies successes in commercial applications of crowdsourcing, and argues that crowdsourcing intelligence provides greater degrees of penetration and persistence in community surveillance, and is more attuned to detecting subtle signs masked within a local context. He then provides recommendations on building and sustaining a wide base of motivated and committed users in order to refine existing nation-wide initiatives into effective intelligence crowdsourcing platforms. MAJ Ng feels that the effective implementation of crowdsourcing as a novel intelligence tool will not only enhance intelligence collection on lone-wolf terrorism, but also engender a stronger sense of ownership for homeland security among the citizens, and project a tougher deterrence stance against terror networks.

In the essay, 'Survivability of a Smart Nation', ME6 Calvin Seah Ser Thong, highlights that in this age of technology, the trend of cyber attacks is ever increasing and, no nation is spared. Even in Singapore, it has been reported that 16 waves of targeted cyber attacks have been surfaced to the Cyber Security Agency of Singapore from April 2015 to June 2016. More recently, two waves of cyber attacks disrupted StarHub's broadband network in October 2016. On both occasions, subscribers' bug-infected machines turned into zombie machines that carried out distributed denial-of-service attacks on StarHub's network. Following these attacks, security experts have warned that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. ME6 Seah says that as Singapore embarks on the Smart Nation initiative to transform itself into the world's first true Smart Nation, there could potentially be a Centre of Gravity that could pose as a critical vulnerability. ME6 Seah explores this notion by firstly examining Singapore's Smart Nation Initiative. Next, he examines Clausewitz's Centre of Gravity concept and explores whether the Information and Communications Network can become the Centre of Gravity of a 'Smart Nation'. Finally, ME6 Seah proposes recommendations to bolster a Smart Nation's security by adopting Dr David Wilkes' Survivability Onion, a five-layer defence to mitigate against any potential threats.

The essay, 'Hybrid Warfare – A Low-Cost High-Return Threat to Singapore as a Maritime Nation' is written by MAJ Bertram Ang Chun Hou. MAJ Ang feels that the advent of hybrid warfare has raised concerns

for Singapore with the potential challenges that it may bring. Being a nation surrounded by water on all sides with no natural resources, maritime trading has not only become a way to maintain sustenance, but a key contributor to Singapore's economy. An attack on Singapore's maritime sector would not only affect its way of life, but undermine shipping and erode confidence in Singapore as a transhipment hub. While the SAF is already well-prepared against a conventional threat, a hybrid threat can inflict equal or even more damage than any conventional means and, at a lower cost to the adversary. In this essay, MAJ Ang discusses the vulnerabilities in Singapore's maritime domain, and how an aggressor could exploit this through hybrid means, evading the SAF's conventional defence methods. The rationale behind a potential aggressor attacking Singapore through the maritime domain is also deliberated, providing examples as to how maritime sabotage could affect the populace in Singapore. MAJ Ang also scrutinises various hybrid methods while explaining the ineffectiveness of responding through conventional means to a hybrid threat. Lastly, MAJ Ang provides recommendations on how the SAF can augment the Republic of Singapore Navy (RSN) to better combat hybrid threats.

According to MAJ(NS) Tan Kok Yew who wrote, 'Winning Hearts through Communication – A Social Media Engagement Strategy for the Military', with the high social media penetration rate in Singapore, it would be beneficial if a model to engage military personnel through the Social Media could be promulgated to guide commanders, human resource managers and communication practitioners. In this essay, MAJ(NS) Tan combines a military retention framework derived from civilian employee retention models and gaps in existing military employee retention frameworks, applying it to Social Media strategies to devise a Social Media engagement model to propose an enhancement to military employee retention in the SAF. He proposes the POWERS framework to provide the first step towards an effective employee retention model for the SAF.

In 'Beyond SAF50: Maintaining the SAF's Edge amidst Global, Regional and Domestic Challenges', MAJ James Yong Dun Jie explores the various difficulties facing the SAF as it moves beyond its 50th anniversary. MAJ Yong highlights that while the SAF has undoubtedly served its purpose in deterring potential adversaries for the past five decades, it has also allowed Singapore to gain the confidence of foreign nations, resulting in continued economic growth. In addition, the participation of the SAF in multinational operations has also forged partnerships with countries, which promoted the growth of defence diplomacy. All these were attributed to Singapore's ability to react to the ever-changing strategic landscape thus far. In this essay, MAJ Yong analyses the emerging trends from the three domains—global, regional and domestic—and the potential challenges that may dull the SAF's edge. With the rise of hybrid warfare, geopolitical tensions, alongside a shrinking population, MAJ Yong discusses how the aforementioned factors could impact Singapore, and offer recommendations on how the SAF can remain relevant to national defence as well as to act as a stabilising anchor for Singapore.

In the essay entitled, 'Unmanned Aerial Vehicles – A Clear and Present Danger and What We Can Do About Them', MAJ Jerry Chua examines how Unmanned Aerial Vehicles (UAV) have transformed into a deadly weapon that is utilised by both military and terrorists. According to MAJ Chua, there is no single solution to deal with the threat posed by UAVs in hostile hands. Possible defence concepts such as geo-fencing, high energy lasers and jamming may still not succeed. MAJ Chua then proposes a multi-layered approach in dealing with UAVs to provide for contingencies in the event that one layer fails. This five-layer defence model comprise the concepts of Prevention, Deterrence, Denial, Detection and Destruction/Interruption. With this model, MAJ Chua discusses how Singapore can prevent attacks from UAVs and instead, plan a counterattack against the aggressor.

We would like to wish all our readers happy reading for the holiday season. Have a Merry Christmas and Happy New Year 2019!

The POINTER Editorial Team

ENDNOTES

1 https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2018/october/04oct18_speech2

CROWDING OUT THE LONEWOLF – CROWDSOURCING INTELLIGENCE TO PREVENT LONEWOLF ATTACKS

by **MAJ Jeffrey Ng Zhao Hong**

Abstract:

With terrorist networks turning toward lonewolf attacks as their choice modus operandi, homeland security forces are quickly realising that traditional top-down surveillance programmes are ill-suited to detect the subtle indicators of sporadic attacks perpetrated by legal residents with no known links with terrorist cells. This essay studies successes in commercial applications of crowdsourcing, and argues that crowdsourcing intelligence provides greater degrees of penetration and persistence in community surveillance, and is more attuned to detecting subtle signs against the local context. It then provides recommendations on building and sustaining a wide base of motivated and committed users in order to refine existing nation-wide initiatives into effective intelligence crowdsourcing platforms. The effective implementation of crowdsourcing as a novel intelligence tool will not only enhance intelligence collection on lone-wolf terrorism, but also engender a stronger sense of ownership for homeland security among the citizens, and portray a tougher deterrence stance against terror networks.

Keywords: Surveillance; Subtle; Penetration; Community; Deterrence

INTRODUCTION

> *"The most likely scenario that we have to guard against right now ends up being more of a lone wolf operation than a large, well-coordinated terrorist attack."*
>
> *- Barack Obama, 44th President of the United States of America.*[1]

On the evening of 14th July, 2016, a rented 19-tonne cargo truck rampaged through the crowds of revellers celebrating Bastille Day on the Promenade des Anglais in Nice, France, taking the lives of 86 people and injuring 434 others.[2] What seemed like an accident at first turned out to be a devastating lonewolf attack, planned and executed by a single person—Mohamed Lahouaeij-Bouhlel, a legal Tunisian resident in France. Subsequent investigations revealed that Lahouaeiji had become radicalised shortly before the attack, consulting websites carrying jihadist propaganda and expressing extremist views.[3] His friends noticed him growing a beard eight days before the attack and began showing them Islamic State of Iraq and Syria (ISIS) beheading footages in his phone, claiming that he had grown accustomed to such videos. Days before the attack, Lahouaeiji also persuaded some friends to smuggle large amounts of cash back to his family in Tunisia when previously he only sent small sums at regular intervals.[4] With the benefit of hindsight, these signs should have been

obvious red flags to the French intelligence agencies. However, unless Lahouaeiji had already been pre-identified as a high-risk individual, such subtle tell-tale signs of an impending lonewolf attack could hardly be detected by routine surveillance programmes. Such is the challenge of tracing and preventing a lone-wolf attack. With lonewolf attacks becoming more common and deadlier, homeland security forces have quickly realised that traditional top-down intelligence approaches, such as electronic surveillance, are ill-suited for detecting and preventing lonewolf operations as such operations often involve a single individual with little communication with the outside world on his attack plan.[5] This essay argues that a bottom-up approach involving the local community's participation through crowdsourcing could be an effective alternative to collect tell-tale signs of a brewing lonewolf attack, and could have the spin-off benefit of strengthening the citizenry's sense of ownership for homeland security. It also provides suggestions for transforming existing nation-wide initiatives into effective intelligence crowdsourcing platforms.

THE EMERGENCE OF THE LONEWOLF CHALLENGE

The global security landscape was irrevocably altered following the iconic terrorist attacks waged on United States (US) home soil on 11th September, 2001. The collapse of the twin World Trade towers solidified the resolve of the civilised world and motivated an international military campaign against the perpetrator of this hideous crime. Dubbed the 'War on Terror', the protracted military campaign relentlessly targeted the top dogs within the Al-Qaeda hierarchy and significantly withered their assets and communications capabilities. While the War on Terror succeeded in neutralising Al-Qaeda's central hierarchy, it inadvertently pressured Al-Qaeda into evolving its tactics to one where it rallied individuals at the lowest level, with minimal contact with its reduced command structure.[6] More critically, the protracted War on Terror supplied ample footages of the injustices waged by the US and the West on the Muslim community, providing fertile ground for Al-Qaeda and its splinter groups to cultivate a ready base of aggrieved individuals into lonewolf jihadists.[7] Instead of investing resources into scouting, recruiting and training operatives, this rudimentary form of crowdsourcing allows the terrorist group to reach out to a wider population of would-be jihadists with little monetary and time investments while staying under the radar of surveillance programmes by negating the need for two-way communications. Noting the advantages of inciting lonewolf attacks, ISIS has become more prolific over the years in packaging its propaganda and making use of existing social media platforms to appeal to the young and impressionable minds. In September 2014, Abu Muhammad al-Adnani, the official spokesman for ISIS, urged followers and sympathisers to "kill in any manner...a disbelieving American or European—especially the spiteful and filthy French—or an Australian, or a Canadian or any other disbeliever."[8]

United Airlines Flight 175 explodes after crashing into the South Tower of the World Trade Centre.

As compared to yesteryears, the indoctrination of potential lonewolf operatives is given an additional boost by the use of the Internet and social media platforms as broadcast channels. In place of books, newsletters and manifestos, the speed and reach of the Internet today have enabled worldwide consumption of terroristic ideologies and methods by individuals in anonymity.[9] Disenfranchised individuals can easily scour accessible websites and online videos to reinforce their burgeoning beliefs, chat anonymously with like-minded individuals, and acquire tools and methods needed to perform mass murders. With the ease of accessibility to resources and guidance online, lone-wolf attacks can be easily hatched, planned, and executed all by a single individual in a short span of time with little communication.

These unique characteristics of lonewolf operations render traditional intelligence collection methods impotent.[10] As aptly described by the Head of Counter-Terrorism for the New York Police Department, "If the conspiracy to commit a terrorist act is a conspiracy of one, and the planning for that is unsophisticated...and is only happening in the mind of the offender, from an intelligence standpoint... that's very hard to detect."[11] Indeed, even invasive electronic surveillance is only viable if targeted at an already identified suspect, and it would be extremely resource-intensive and unsustainable for any intelligence agency to analyse every single Tweet, Facebook post and email floating in the cyberspace to sniff out early indicators. Hence, such means are unlikely to aid in the initial identification of potential individuals. Besides electronic surveillance, traditional human intelligence activities could be challenging without a clear hierarchy or structure to assign spies for monitoring and espionage. Community outreach programmes aimed at garnering domestic intelligence have also seen limited effectiveness. As such programmes depend on personal interaction between law enforcer and the citizens, they are resource-intensive, and often suffer from limited reach, especially to individuals who are less visible, less accessible and more resistant to interacting with the figures of authority.[12] Limited penetration and persistence prevent such programmes from picking up day-to-day signs and indicators of an individual's early step toward self-radicalisation, such as Lahouaeij's sudden mosque attendance and growing of a beard.

With law enforcers and the intelligence community on the back foot against lone-wolf attacks, it is no surprise that terrorist groups have been able to lay claims to an increasing number of such attacks. From mid-2015 to mid-2016 alone, there were nine attacks in the West—ranging from a mass shooting by a single disguised tourist at a packed tourist beach, killing 38 and injuring 39 others to Lahouaeij's truck attack on Bastille Day in Nice.[13] The latest instalment to this ongoing trend involved yet another truck rampaging through a Christmas Market in Berlin, killing a dozen people.[14]

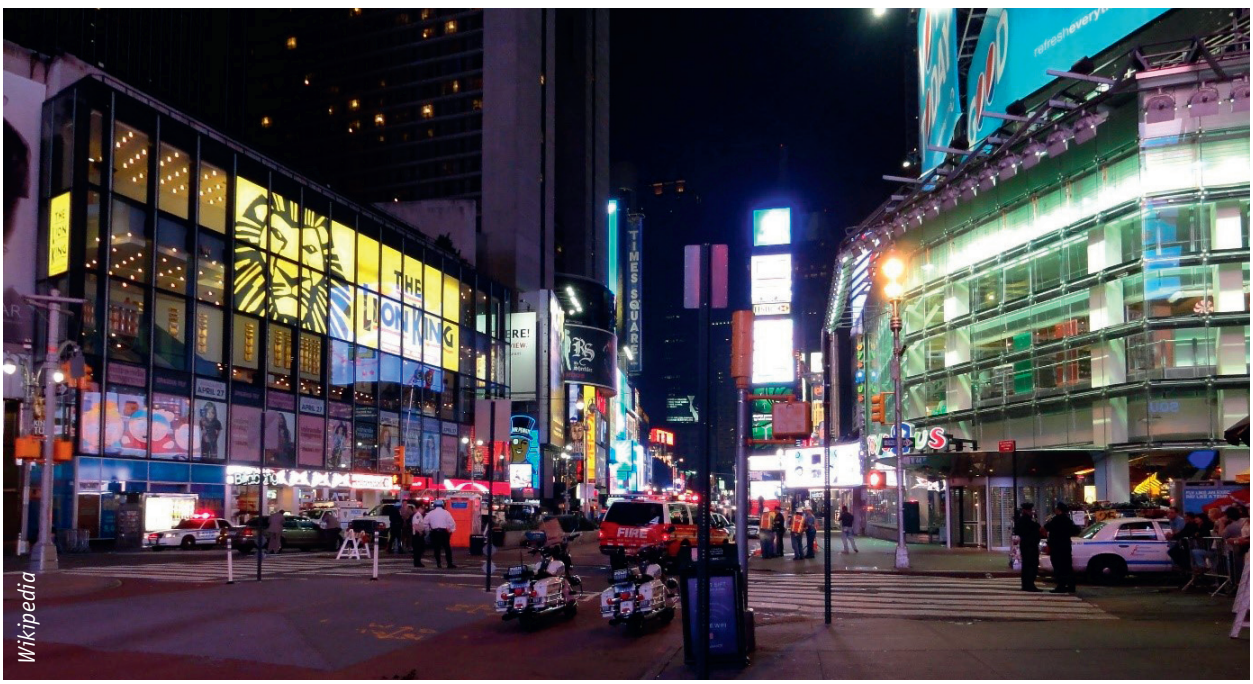
VALUE PROPOSITIONS FOR CROWDSOURCING DOMESTIC INTELLIGENCE

The continuing onslaught of lone-wolf attacks is a worrying trend, and the repeated success of similar modus operandi (e.g., mass shooting by a lone gunman, or a truck rampaging through revellers) underscores the inadequacy of current top-down intelligence approaches in preventing such tragedies. With the intelligence community seemingly at its wits' end, parallels could be drawn from commercial arenas to better understand and appreciate the value propositions of adopting crowdsourcing as a bottom-up, community-based intelligence approach.

The term 'crowdsourcing' was first coined by Jeff Howe, and was later defined by Daren Brabham as 'an

online, distributed problem solving and production model that leverages the collective intelligence of online communities to serve specific organisational goals.'[15] Crowdsourcing differs from outsourcing in that it involves the participation of masses, instead of a single assigned entity. The concept of leveraging on the wisdom of crowds is not a new one. In fact, Francis Galton had already demonstrated the strength of collective wisdom more than a century ago in 1907. At a crowded country fair, Galton held a contest where he had 800 people guess the weight of a slaughtered and dressed ox. While no one individually knew the weight of the dead ox, the median of their individual guesses was more accurate than any of the cattle experts' estimates solicited separately from the crowd.[16] While Galton had to physically gather a crowd, crowdsourcing in the 21st century could easily reach millions by riding on the Internet and popular social media platforms.

In the present day, the strength of crowdsourcing information had already been harnessed to a great utility in commercial applications. Leveraging on traffic information supplied by road users, Waze, a mobile navigation application for use on smartphones, is able to provide accurate real-time information on traffic flow, congestions, road conditions and obstructions, accidents, and even ad-hoc speed traps.[17] Another successful case study was the Defense Advanced Research Projects Agency's (DARPA) Ten Red Balloons experiment held in December 2009. In a contest for a $40,000 prize, teams had to locate ten red balloons randomly placed around the US. The winning team from Massachusetts Institute of Technology (MIT) located all ten balloons in less than nine hours, a task which DARPA had originally estimated would take approximately two weeks.[18] Riding on Twitter and by developing a pyramid reward scheme where rewards were given to the ones who supplied the balloons' locations and also to the ones who referred the balloon finders, the team was able to quickly establish a self-propagating base of motivated and involved users. The speed and accuracy in which this task was accomplished reinforced the effectiveness



Police cordoned off Times Square after finding a bomb in a car.

of distributed problem-solving for scenarios that are directly applicable to intelligence gathering.

With the ease of accessibility to resources and guidance online, lone-wolf attacks can be easily hatched, planned, and executed all by a single individual in a short span of time with little communication.

Applying crowdsourcing to the domain of security and intelligence collection might seem counter-intuitive at first glance, as the intelligence value of information is often associated with the confidentiality of its source, and limited exposure to the public. However, history is replete with examples where information volunteered by the public, in the form of tip-offs, had been crucial to thwarting lone-wolf terrorist plots. For example, the Times Square bombing in 2010 was averted when a local street vendor alerted two New York policewomen on street patrol to a smoking Sport Utility Vehicle (SUV).[19] Real-world events like these are testament to the utility of citizen intelligence in preventing lone-wolf terrorism.

In fact, a bottom-up, community-based intelligence gathering approach offers at least three direct advantages over traditional top-down surveillance methods in detecting and preventing lonewolf attacks. Firstly, mobilising the entire citizen taps into a much wider pool of resources, as compared to the limited manpower resources employed by law enforcement agencies. This allows the collection effort to grow exponentially in coverage, and provides more pervasive surveillance without the need for investments in invasive technology. The pervasiveness is necessary for picking up subtle signals which are often emitted by lonewolf terrorists. An analysis of past case studies indicated that although limited, lonewolves do possess networks, and often provide clues to their violent intents in some form or manner, and these will more likely be noticed by local citizens within the lonewolf's community, as compared with national surveillance efforts.[20]

Closely linked to the advantage of pervasiveness is the advantage of persistence in a collection. Compared to community outreach programmes where law enforcers have limited touch-points with a small subset of individuals, motivated citizens are constantly embedded in the community, and can provide conscious observations of their surroundings and their fellow citizens at least 16 hours a day. This day-to-day persistence is important for painting a reliable baseline against which any subtle changes in behaviours, demeanours or ideologies could be detected as signals of a self-radicalisation process.[21]

The third advantage of involving the local community is local expertise, which is important in filtering abnormalities from normalcy. Law enforcers who are not an integral part of the local community could have difficulty in noticing out-of-norm practices. In addition, as compared to locals in the same neighbourhood, law enforcers are often seen as figures of authority and are less likely to receive unsolicited and unguarded information.

Other than these direct advantages, a bottom-up approach, through encouraging direct participation by the local communities, could provide an indirect advantage of strengthening the sense of ownership among the citizens for the fight against terrorism. By involving the citizens and motivating them to proactively provide useful information, a ground-up crowdsourcing initiative could ingrain in them the notion that everyone, and not just the law enforcers, has a part to play in preventing terrorism. With the entire nation mobilised against lone-wolf terrorism, a stronger deterrence stance is portrayed.

A police officer speaking to a group of children in Des Moines, Iowa.

MAKING CROWDSOURCING WORK

The advantages of mobilising the entire nation against terrorism have not gone unnoticed by Singapore's homeland security forces. In the latest effort to strengthen the nation's resilience against a terrorist attack, a new national movement named SGSecure was officially launched in September 2016.[22] At the launch, PM Lee Hsien Loong highlighted that everyone should be a 'prepared citizen' by learning how to protect themselves and their families, and also by learning how to recognise signs of suspicious behaviours, identify suspicious items, and report it to the authorities. As part of this campaign, an SGSecure mobile application was also unveiled, providing members of the public with a one-stop portal to receive alerts during national emergencies, and also for them to provide information to the authorities. Such a mobile application is a step in the right direction as it provides a platform for citizens to provide bottom-up information. However, other law enforcement agencies abroad have also developed similar online portals and mobile applications and yet most have failed to provide tangible enhancements to domestic intelligence collection. The SGSecure mobile application could take reference from commercial crowdsourcing successes, and enhancements such as incorporating two-way communication with the users, infusion of elements of fun as a form of intrinsic motivation, and the provision of tangible rewards as a form of extrinsic motivation.

In comparison with Waze, or other commercial applications, crowdsourcing intelligence faces an uphill battle of amassing and retaining a ready pool of public users, especially if the threat of terrorism is

not clear and present in the public's consciousness. A series of contests with tangible rewards, similar to the DARPA's Ten Red Balloons experiment, could be initiated to generate interests and publicity in order to create the initial user base. This could also serve to validate the effectiveness of the mobile platform in coping with the online traffic, and also provide an indication of how useful crowdsourcing domestic intelligence could be in a local real-world context.

With the intelligence community seemingly at its wits' end, parallels could be drawn from commercial arenas to better understand and appreciate the value propositions of adopting crowdsourcing as a bottom-up, community-based intelligence approach.

Beyond the initial hype, we will need to sustain the public's involvement in this nation-wide intelligence collection effort. To do so, a two-way engagement is crucial as the citizens need to feel involved as part of the overall intelligence programme.[23] Without feedback on the actions that have been taken following the submission of a report, the citizens would feel less inclined to provide information in the future. In addition, transparency in the follow-up action would reinforce the notion that the citizens are treated as part of the nationwide effort, and not just an additional conduit of intelligence. Most of the existing applications, including SGSecure, fail to provide a clear and personal feedback to the citizen, and hence fail to elicit repeated interactions. In addition, a two-way engagement could also manifest as requests for further information by the law enforcement agencies. For example, if the police require more information regarding a suspicious red vehicle, this could be pushed out to the public using the mobile application, and the public could be encouraged to provide any details with regard to this vehicle. In this way, stronger public involvement could be engendered.

Another crucial ingredient in successful crowdsourcing is a strong sense of commitment by the users. This could be engendered by a combination of intrinsic and extrinsic motivators. Taking a leaf from Waze's success story, a collection of virtual rewards, such as points, levels, badges and avatars, could be awarded to members of the public who provide useful pieces of information. These forms of gamification, 'the use of game thinking and game mechanics in non-game contexts to engage users in solving problems,' provide recognition to the users' contributions, and positively reinforce their commitment to the task, thereby spurring on further participation.[24] Linking this to popular social media platforms, such as Facebook and Twitter accounts, could also help to personalise the achievements, and also help reach out to a wider base of participation.[25] Other than superficial game mechanics, actual monetary rewards could also be a very strong motivator for repeated contributions. However, studies have found that tasks that are framed with intrinsic rewards and altruistic causes, such as helping others, have been found to be associated with higher work quality.[26] In the context of intelligence gathering to prevent lone-wolf attacks, a clear case for altruism and community self-protection is present. Hence, in combining intrinsic and extrinsic motivators, the use of intrinsic motivators should be weighted more heavily to avoid negative backlash in the public's sentiments.

Other than interactivity and reinforcements, successful crowdsourcing for intelligence should also include mechanisms where spurious information could be weeded out without heavy investments in intensive data analysis. This could take the form of peer review,

where members of public provide authentication or validation of the information posted by other members. This could also avoid overcrowding of data, and provide a means to prioritise follow-up actions by security forces. With the appropriate reinforcement mechanisms in play, the online community could potentially self-police the quality and validity of information provided.

Without feedback on the actions that have been taken following the submission of a report, the citizens would feel less inclined to provide information in the future.

CONCLUSION

With the rise of regional terror threat, and the proclamation by ISIS to establish a caliphate in our region, Singapore has to maintain constant vigilance against the threat of terrorism. With terrorist groups evolving their tactics to one where disenfranchised individuals are insidiously motivated to perform sporadic acts of terror, traditional top-down surveillance programmes will be less effective in picking up subtle signs and clues exhibited by self-radicalised individuals. To guard against 'crowdsourced' terrorism, a novel bottom-up intelligence gathering approach is needed. A well-designed, centralised crowdsourcing platform could serve as a one-stop portal for citizens to provide bottom-up intelligence to homeland security agencies for quick and responsive thwarting of potential lone-wolf attacks. The launch of the SGSecure national movement serves to build a strong foundation for such a crowdsourcing initiative by highlighting the threat of terrorism in the public's consciousness. With the correct mix of intrinsic and extrinsic motivators, coupled with the right dosage of publicity and public education, crowdsourcing domestic intelligence would prove to be a viable strategy in detecting and preventing lonewolf terrorism, and in strengthening the nation's vigilance against terrorism.

BIBLIOGRAPHY

AFP, "What do we know about the Nice attacker?" *The Local*, July 17, 2016, accessed February 18, 2017, http://www.thelocal.fr/20160717/nice-attacker-body-building-drug-taking-womanising.

Bakker, Edwin, and Beatrice de Graaf. "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed", *Perspectives on Terrorism*, 5 (2011): 5-6.

Bates, Rodger A., "Dancing with Wolves: Today's Lone Wolf Terrorists", *The Journal of Public and Professional Sociology*, 4 (2012): 1-14.

Bergen, Peter, "Why It's So Hard to Track a 'Lone Wolf'," *Spiegel Online*, June 17, 2016, accessed February 17, 2017, http://www.spiegel.de/international/world/the-danger-of-lone-wolf-terrorists-like-omar-mateen-a-1098263.html.

Brabham, Daren, *Crowdsourcing*, Cambridge, MA: MIT Press, 2013.

Chia, Lianne. "SGSecure launched to prepare public for terror attacks," *Channel Newsasia*, September 24, 2016, accessed February 17, 2017, http://www.channelnewsasia.com/news/singapore/sgsecure-launched-to-prepare-public-for-terror-attacks/3150566.html.

Coultas, Bryan T., Crowdsourcing intelligence to combat terrorism: harnessing bottom-up collection to prevent lone-wolf terror attacks, Diss. Monterey, California: *Naval Postgraduate School*, 2015.

Deterding, Sebastian, Dan Dixon, Rilla Khaled, and Lennart Nacke. "From Game Design Elements to Gamefulness: Defining 'Gamification'.", *Proceedings of the 15th International Academic MindTrek Conference*, Tampere, Finland: Mindtrek (2011): 10, https://www.cs.auckland.ac.nz/courses/compsci747s2c/lectures/paul/definition-deterding.pdf.

Empson, Rip. "WTF is Waze and Why did Google Just Pay a Billion+ for It?" *TechCrunch*, June 11, 2013, accessed February 18, 2017, https://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/.

Ford, Christopher M. "Twitter, Facebook and Ten Red Balloons: Social Network Problem-Solving and Homeland Security," *Homeland Security Affairs*, 7 (2011), accessed

February 18, 2017, https://www.hsaj.org/articles/54.

Furchgott, Roy, "Filling in Map Gaps with Waze Games," *The New York Times*, May 6, 2010, accessed February 17, 2017, https://wheels.blogs.nytimes.com/2010/05/06/filling-in-the-map-gaps-with-waze-games/?_r=0.

Gendar, Alison, and Rocco Parascandola. "Time Square car bomb: Cops evacuate heart of NYC after 'potential terrorist attack'," *Daily News*, May 2, 2010, accessed February 16, 2017, http://www.nydailynews.com/news/crime/time-square-car-bomb-cops-evacuate-heart-nyc-potential-terrorist-attack-article-1.444423.

Gerges, Fawaz, The Rise and Fall of Al-Qaeda. Oxford: *Oxford University Press*, 2011.

Gomez, Alan. "Berlin attack latest in disturbing terror trend," *USA Today*, December 20, 2016, accessed February 18, 2017, http://www.usatoday.com/story/news/world/2016/12/20/berlin-attack-terror-trend-lone-wolf/95661116/.

Hays, Tom. "Lone-Wolf Terror Threat Focus of NYPD Conference," *ABC News*, November 6, 2014, accessed 17 February 2017, http://abcnews.go.com/U.S./wireStory/lone-wolf-terror-threat-focus-nypd-conference-26746906.

Howe, Jeff. "The Rise of Crowdsourcing," *Wired Magazine*, June 01, 2006, accessed February 18, 2017, https://www.wired.com/2006/06/crowds/.

Lister, Tim. "Why the threat of 'lone wolf' attacks looms large in Australia," *CNN*, December 16, 2014, accessed February 17, 2017, http://edition.cnn.com/2014/12/15/world/lister-australia-terror/.

Love, Brian, and Robert-Jan Bartunek. "Timeline: The Bastille Day attack in Nice," *Reuters*, July 17, 2016, accessed February 18, 2017, http://www.reuters.com/article/us-europe-attacks-nice-timeline-idUSKCN0ZX0GA.

MacInnis, Laura, "Obama says "lone wolf terrorism" biggest U.S. threat," *Reuters*, August 16, 2011, accessed February 18, 2017, http://www.reuters.com/article/us-usa-obama-security-idUSTRE77F6XI20110816.

Morgan, Tom, Chazan, David and Turner, Camilla, "Nice killer Mohamed Lahouaiej Bouhlel 'only started going to mosque this April'," *The Sydney Morning Herald*, July 17, 2016, accessed February 18, 2017, http://www.smh.com.au/world/nice-killer-mohamed-lahouaiej-bouhlel-only-started-going-to-mosque-this-april-20160717-gq7esi.html.

Polden, Jake. "Timeline of terror: The deadly attacks on the West in the last 12 months as gunman goes on a rampage through German shopping mall and kills nine people," *Mail Online*, July 24, 2016, accessed 17 Feburary, 2017, http://www.dailymail.co.uk/news/article-3703884/Timeline-terror-deadly-attacks-West-12-months.html.

Rogstadius, Jakob, Kostakos, Vassilis, Kittur, Aniket, Smus, Boris, Laredo, Jim and Vukovic, Maja, "An Assessment of Intrinsic and Extrinsic Motivation on Task Performance in Crowdsourcing Markets," *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media* (2011), http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2778/3295, 321.

Skolnick, Jerome H., and Bayley, David H., "Community Policing: Issues and Practices Around the World," *National Institute of Justice: Issues and Practices*, (1988), 1-86, https://www.ncjrs.gov/pdffiles1/Digitization/111428NCJRS.pdf.

Teich, Sarah, "Trends and Developments in Lone Wolf Terrorism in the Western World: An Analysis of Terrorist Attacks and Attempted Attacks by Islamic Extremists," *International Institute for Counter-Terrorism*, October 2013, 22, accessed February 18, 2017, http://www.ctcitraining.org/docs/LoneWolf_SarahTeich2013.pdf.

Worth, Katie. "Lone Wolf Attacks Are Becoming More Common — And More Deadly," *Frontline*, July 14, 2016, accessed February 18, 2017, http://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

Zorff, Lior, Mindsharing: The art of Crowdsourcing Everything, New York, NY: *Penguin Publishing Group*, 2015.

ENDNOTES

1. Laura MacInnis, "Obama says "lone wolf terrorism" biggest U.S. threat," *Reuters*, August 16, 2011, accessed February 18, 2017, http://www.reuters.com/article/us-usa-obama-security-idUSTRE77F6XI20110816.
2. Love, Brian Love and Robert-Jan Bartunek, "Timeline: The Bastille Day attack in Nice," *Reuters*, July 17, 2016, accessed February 18, 2017, http://www.reuters.com/article/us-europe-attacks-nice-timeline-idUSKCN0ZX0GA.
3. AFP, "What do we know about the Nice attacker?", *The Local*, July 17, 2016, accessed February 18, 2017, http://www.thelocal.fr/20160717/nice-attacker-body-building-drug-taking-womanising
4. Morgan, Tom, Chazan, David and Turner, Camilla, "Nice killer Mohamed Lahouaiej Bouhlel 'only started going to mosque this April' ", *The Sydney Morning Herald,* July

17, 2016, accessed February 18, 2017, http://www.smh.com.au/world/nice-killer-mohamed-lahouaiej-bouhlel-only-started-going-to-mosque-this-april-20160717-gq7esi.html.

5. Worth, Katie "Lone Wolf Attacks Are Becoming More Common — And More Deadly," *Frontline*, July 14, 2016, accessed February 18, 2017, http://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

   Bergen, Peter "Why It's So Hard to Track a 'Lone Wolf", *Speiegel Online*, June 17, 2016, accessed February 2017, http://www.speiegel.de/international/world/the -danger-of-lone-wolf-terrorists-like-omar-mateen-a-1098263.html

6. Gerges, Fawaz, *The Rise and Fall of Al-Qaeda* (Oxford: *Oxford University Press*, 2011), 95, 152.

7. Ibid, 161-164.

8. Lister, Tim, "Why the threat of 'lone wolf' attacks looms large in Australia," *CNN*, December 16, 2014, accessed February 17, 2017, http://edition.cnn.com/2014/12/15/world/lister-australia-terror/.

9. Bates, Robert A.,"Dancing with Wolves: Today's Lone Wolf Terrorists", *The Journal of Public and Professional Sociology*, 4 (2012): 4.

10. Bakker, Edwin and de Graaf, Beatrice "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed," *Perspectives on Terrorism*, 5 (2011): 5-6.

11. Hays, Tom, "Lone-Wolf Terror Threat Focus of NYPD Conference," *ABC News*, November 6, 2014, accessed 17 February 2017, http://abcnews.go.com/U.S./wireStory/lone-wolf-terror-threat-focus-nypd-conference-26746906.

12. Skolnick, Jerome H and Bayley, David, "Community Policing: Issues and Practices Around the World," *National Institute of Justice: Issues and Practices*, (1988), 84, https://www.ncjrs.gov/pdffiles1/Digitization/111428NCJRS.pdf.

13. Polden, Jake "Timeline of terror: The deadly attacks on the West in the last 12 months as gunman goes on a rampage through German shopping mall and kills nine people," *Mail Online*, July 24, 2016, accessed 17 Feburary, 2017, http://www.dailymail.co.uk/news/article-3703884/Timeline-terror-deadly-attacks-West-12-months.html.

14. Gomez, Alan "Berlin attack latest in disturbing terror trend," *USA Today*, December 20, 2016, accessed February 18, 2017, http://www.usatoday.com/story/news/world/2016/12/20/berlin-attack-terror-trend-lone-wolf/95661116/.

15. Howe, Jeff "The Rise of Crowdsourcing," *Wired Magazine*, June 01, 2006, accessed February 18, 2017, http://www.wired.com/2006/06/crowds/

    Brabham, Darren, Crowdsourcing (Cambridge, MA: *MIT Press*, 2013): xix.

16. Zorff, Lior Mindsharing: The art of Crowdsourcing Everything, (New York, NY: *Penguin Publishing Group*, 2015), 15.

17. Empson, Rip, "WTF is Waze and Why did Google Just Pay a Billion+ for It?", *TechCrunch*, June 11, 2013, accessed February 18, 2017, https://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/.

18. Ford, Christopher M, "Twitter, Facebook and Ten Red Balloons: Social Network Problem-Solving and Homeland Security," *Homeland Security Affairs*, 7 (2011), accessed February 18, 2017, https://www.hsaj.org/articles/54.

19. Gendar, Alison and Parascandola, Rocco "Time Square car bomb: Cops evacuate heart of NYC after 'potential terrorist attack'," *Daily News*, May 2, 2010, accessed February 16, 2017, http://www.nydailynews.com/news/crime/time-square-car-bomb-cops-evacuate-heart-nyc-potential-terrorist-attack-article-1.444423.

20. Teich, Sarah "Trends and Developments in Lone Wolf Terrorism in the Western World: An Analysis of Terrorist Attacks and Attempted Attacks by Islamic Extremists," *International Institute for Counter-Terrorism*, October 2013, 22, accessed February 18, 2017, http://www.nydailynews.com/news/crime/time-square-car-bomb-cops-evacuate-heart-nyc-potential-terrorist-attack-article-1.444423.

    Hays, Tom, "Lone-Wolf Terror Threat Focus of NYPD Conference," *ABC News*, November 6, 2014, accessed 17 February 2017, http://abcnews.go.com/U.S./wireStory/lone-wolf-terror-threat-focus-nypd-conference-26746906.

21. Coultas, Bryan "Crowdsourcing Intelligence to Combat Terrorism: Harnessing Bottom-up Collection to Prevent Lone-Wolf Terror Attacks.", Master of Arts (Security Studies), *Naval Postgraduate School*, 2015, https://www.hsdl.org/?abstract&did=765304

22. Chia, Lianne, "SGSecure launched to prepare public for terror attacks," *Channel Newsasia*, September 24, 2016, accessed February 17, 2017, http://www.channelnewsasia.com/news/singapore/sgsecure-launched-to-prepare-public-for-terror-attacks/3150566.html.

23. Howe, Jeff "The Rise of Crowdsourcing," *Wired Magazine*, June 01, 2006, accessed February 18, 2017, http://www.wired.com/2006/06/crowds/

24. Deterding, Sebastian, Dixon, Khaled, Rilla, and Nacke, Lennart, "From Game Design Elements to Gamefulness: Defining 'Gamification'." *Proceedings of the 15th International Academic MindTrek Conference*,Tampere, Finland: Mindtrek (2011): 10, https://www.cs.auckland.ac.nz/courses/compsci747s2c/lectures/paul/definition-deterding.pdf.

25. Furchgott, Roy "Filling in Map Gaps with Waze Games," *The New York Times*, May 6, 2010, accessed February 17, 2017, https://wheels.blogs.nytimes.com/2010/05/06/filling-in-the-map-gaps-with-waze-games/?_r=0

26. Rogstadius, Jakob, Kostakos, Vassilis, Kittur, Aniket, Smus, Boris, Laredo, Jim and Vukovic, Maja, "An Assessment of Intrinsic and Extrinsic Motivation on Task Performance in Crowdsourcing Markets," *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media* (2011), http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2778/3295, 321.

MAJ Jeffrey Ng Zhao Hong is a Unmanned Aerial Vehicle (UAV) Pilot by training and is currently attending the United States Air Command and Staff College to further his professional development. Prior to this, he has contributed in command and staff appointments as Flight Commander in 119 SQN and Staff Officer in Air Plans Department. MAJ Ng holds a Bachelors in Psychology from University College London (UCL) and a Masters in Performance Psychology from the University of Edinburgh.

SURVIVABILITY OF A SMART NATION

by **ME6 Calvin Seah Ser Thong**

Abstract:

In this age of technology, the trend of cyber attacks is ever increasing and, no nation is spared. Even in Singapore, it has been reported that 16 waves of targeted cyber attacks have been surfaced to the Cyber Security Agency of Singapore from April 2015 to June 2016. More recently, two waves of cyber attacks disrupted StarHub's broadband network in October 2016. On both occasions, subscribers' bug-infected machines turned into zombie machines that carried out distributed denial-of-service attacks on StarHub's network. Following these attacks, security experts have warned that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. As Singapore embarks on the Smart Nation initiative to transform itself into the world's first true Smart Nation, this could potentially be a Centre of Gravity that could pose as a critical vulnerability. This essay explores this notion by firstly examining Singapore's Smart Nation Initiative. Next, it will look at Clausewitz's Centre of Gravity concept and explore if the Information and Communications Network could become the Centre of Gravity of a 'Smart Nation'. Finally, the essay will propose recommendations to bolster a Smart Nation's security by adopting from Dr David Wilkes' Survivability Onion.

Keywords: Cyber Attacks; Vulnerability; Security; Increasing; Force

INTRODUCTION

> *"Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."*
>
> National Research Council[1]

In February 2016, hackers shut down the internal computer system at the Hollywood Presbyterian Medical Centre for a ransom of almost $3.7 million. The cyber attack forced the centre to revert to paper documentation and to send 911 patients to other hospitals.[2] Communications between physicians and medical staff became bogged down by paper records and doctors' notoriously messy handwriting.[3] Back home, it has been reported that 16 waves of targeted cyber attacks have been surfaced to the Cyber Security Agency (CSA) of Singapore from April 2015 to June 2016.[4] More recently, two waves of cyber attacks disrupted StarHub's broadband network in October 2016. On both occasions, subscribers' bug-infected machines turned into zombie machines that carried out distributed denial-of-service attacks on StarHub's network.[5] Following these attacks, security experts have warned that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. As Singapore embarks on the Smart Nation initiative to transform itself into the world's first true Smart Nation, could this be a Centre of Gravity that could pose as a critical vulnerability? This essay explores this notion by firstly examining Singapore's Smart Nation Initiative. It would next look at Clausewitz's Centre of Gravity concept and explore if the Information and Communications Network could

become the Centre of Gravity of a 'Smart Nation'. Finally, the essay would propose recommendations to bolster a Smart Nation's security by adopting from Dr David Wilkes' Survivability Onion.

SMART NATION INITIATIVE

On 24th November 2014, Prime Minister Lee Hsien Loong launched the Smart Nation Initiative to harness technology to make life better for Singaporeans (*Figure 1*).[7] During the Smart Nation Innovations 2015 event, the Infocomm Development Authority (IDA) of Singapore revealed the development of the Smart Nation Platform consisting of infrastructure and technology to support the roll out of new capabilities to citizens, businesses, and the government. This would eventually enable connectivity across smart, connected devices with applications such as remote health monitoring, remote learning and and even self-driving vehicles.[8] Besides infrastructure and technology, the Big Analytics Skills Enablement initiative has also been announced to equip more people with skills in big data and analytics. As Singapore gears up to be the world's first Smart Nation, it's relying on standards to create a common framework for good practice and to enable innovation. Three key areas that are being trialled are Telemedicine, Urban Living and Urban Mobility. In alignment to the Smart Nation Initiative, MINDEF has also established a committee to chart the way forward to realise our vision of Smart Defence. Within the SAF, data analytics, coupled with predictive engines, will offer sustained sense-making and intelligence to detect security threats to Singapore.

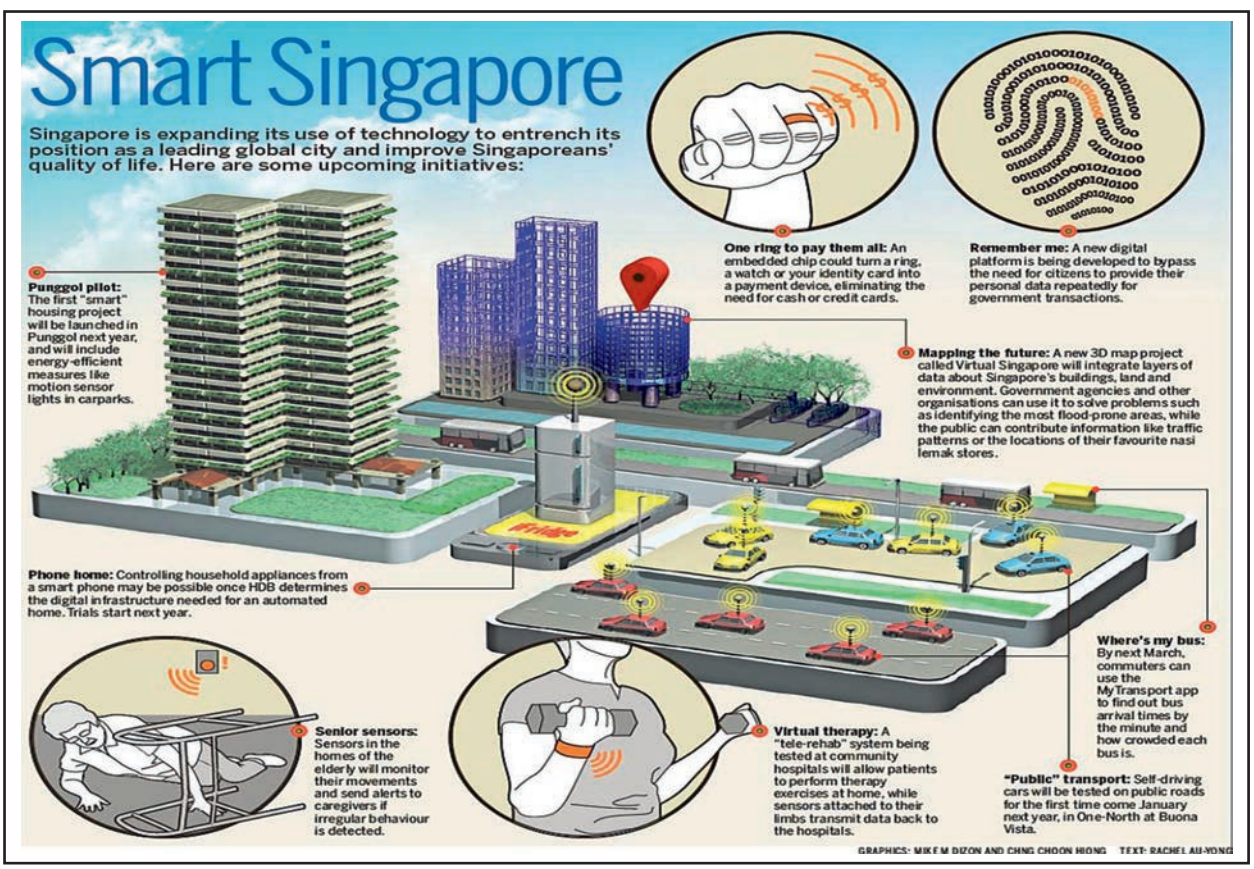


Figure 1: Towards a Smart Nation.[6]

New applications will help streamline corporate services and raise the productivity of administrative and corporate functions. At the individual level, smart technologies will be employed to improve work life in MINDEF.[11]

THE CENTRE OF GRAVITY

The essence of every profession is expressed in the writings of its unifying theorists. For the military, Prussian writer Carl von Clausewitz is regarded as one of the most influential military theorists whose views on the character of war have held up best over the past two centuries.[12] In his book, '*On War*', Clausewitz defined the Centre of Gravity (CoG) as a focal point that if attacked, causes a loss of overall balance. He derived the idea from 19th century physics and believed that it was the key factor in military planning.[13] He surmised that the CoG represents the point where the forces of gravity converge within an object. Thus, striking at the CoG with enough force can cause the object to lose its balance and fall.[14] So, is there a CoG for a Smart Nation that could be a potential vulnerability?

Currently, the 'Cyber' domain that information technology and communication systems depend on is a source of national power.[15] Unlike the traditional domains of air, sea, land and space, it is man created and does not seem to have physical manifestations. Thus, while the infrastructures in the four traditional domains are distinct CoGs that provide lucrative targets for threat vectors, the 'Cyber' domain seems to be devoid of any CoG. But when we study closer, the Clausewitzean principles of key terrain can still be applied to the 'Cyber' domain as it has physical manifestations such as data centres, internet service providers and undersea cables. In his article, 'The key terrain of cyber,' John Mills demonstrates that the 'Cyber' domain has several elements of key terrain that Clausewitz might not have foreseen but would possibly include if he updated his theory of key terrain.[16]

By identifying the CoGs, we can identify sources of power as well as sources of critical vulnerability. Adapting such a bifocal vantage point for a Smart Nation in the areas of critical infrastructure vulnerabilities and the security of the 'Cyber' domain could enable the development of defence mechanisms.[17] Current reality has shown that the more technologically reliant an actor is, the more susceptible they will be to attacks on their information systems. Actors that become reliant on advanced technology may become increasingly vulnerable to issues of friction and fog of war due to the actions of an aggressor perpetuating a cyber war. Attacks would likely not be limited to only military networks and this complicates an actor's capacity to respond as government or, civilian networks may not be as protected nor have the redundancies built into them for a quick recovery.

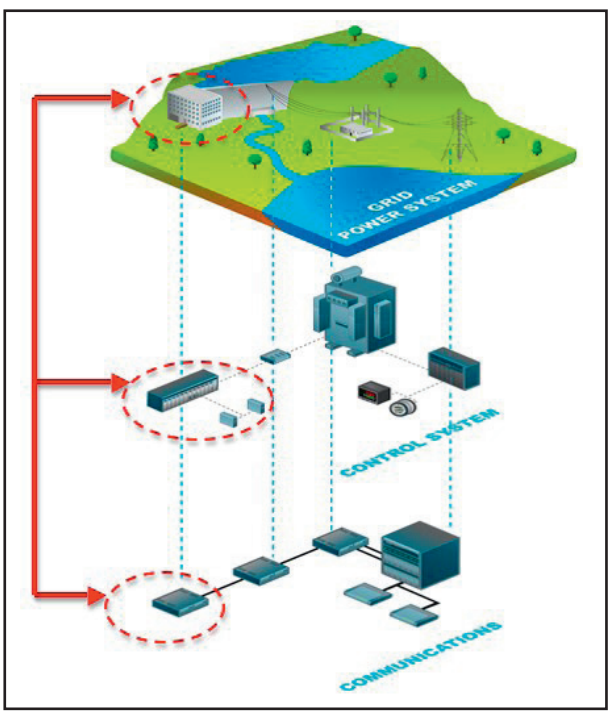


Figure 2: Critical Infrastructure – A potential CoG.[21]

The longer an information based society is disrupted, the greater the damage and public confusion. If the CoG provides for unity within an actor, destroying or degrading this unity can hamper an actor's capacity to engage in effective action within the system.[18] In addition, cyber attacks on national level critical infrastructures such as the energy, transportation and communications sectors could seriously undermine military mission success since the infrastructures are critical in supporting the conduct of military operations (*Figure 2*).[19] In Singapore's context, co-ordinated cyber attacks on critical sectors such as energy, banking and telecommunications can potentially cripple the country, and a Smart Nation with its deep reliance on Infocomm Technology (ICT) will definitely be vulnerable.[20] Furthermore, these cyber attacks may be potential precursors to further military action.

THE 'SMART' BATTLEFIELD

Currently, hackers have yet to actively target smart technologies presumably because not enough electronic devices are connected to the Internet for a cyber attack to be worthwhile. But this situation could change by 2020 when the number of smart devices produced hits an estimated 26 billion units based upon the upward trend of smartphones, Personal Computers (PCs) and tablets use. This could provide the lure for cyber-criminals to begin scouring the technology for weaknesses. What is even more troubling is that smaller smart devices are less likely to have encryption and authentication capabilities due to their limited computing power. It is not just individuals who will be targeted by cyber-criminals; organisations too can be vulnerable when employees bring unsecured smart devices to work.[22] A spate of data breaches at United States (US) companies such as JPMorgan Chase, Home Depot, and Target in 2014 has surfaced questions about the effectiveness of the private sector's information security.[23] A malware code associated with the Russian hacking operation dubbed Grizzly Steppe that was discovered within the system of the US electrical grid's Vermont utility in December 2016 underscores the vulnerabilities of a nation's electrical grid.[24] Power cuts that hit the Ukrainian capital, Kiev due to cyber attacks in 2015 and 2016 prove that utilities can similarly be hacked.[25]

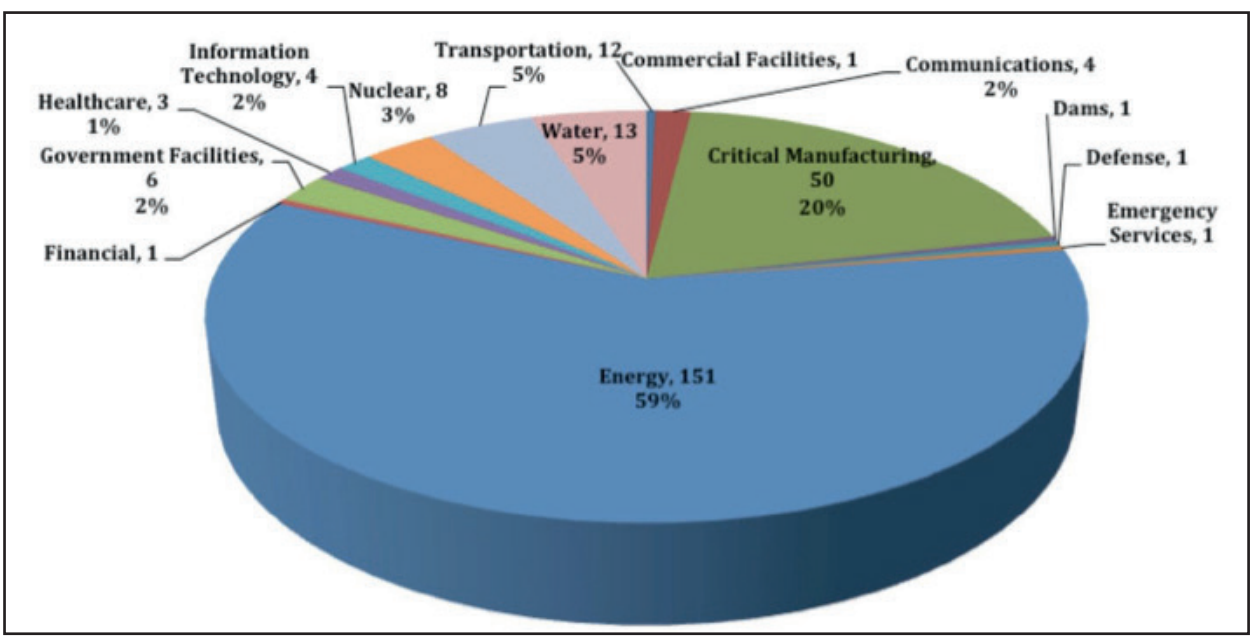


Figure 3: Apportionment of malicious cyber-attacks in 2013.[29]

The cyber attacks on StarHub in October 2016 are reminders of such a reality in Singapore. Following these attacks, security experts warn that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. Mr Alex Tay, Netherlands-based digital security firm Gemalto's Associations of South East Asian Nation (ASEAN) head of identity and data protection has proclaimed that these Internet-connected devices are especially vulnerable as there are no regulations over their security standards. "The lack of consideration for security controls within such devices is giving hackers the ability to take ownership of them," said Mr Tay.[26] For instance, devices such as routers and network cameras have default credentials and passwords that users rarely change. As such, cyber-criminals can turn them into zombie machines that flood targeted systems in a distributed denial-of-service (DDoS) attack.[28]

In a 2013 Monitor report, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) revealed intensification for brute force attacks against control systems mainly belonging to the energy sector (*Figure 3*).[29] Notwithstanding, cyber attacks can even be performed on national infrastructures such as traffic lights. As demonstrated in 2014, Cesar Cerrudo of global security consultancy IOActive, Inc used his laptop to hack Washington City's traffic system. Like his previous tests in Manhattan and elsewhere, Cerrudo was able to turn red lights green and green lights red. He could have unleashed the following scenarios: gridlocking the whole town, turning a busy thoroughfare into a fast-paced highway, paralysing emergency responders, or shut down all roads to the Capitol.[30] Such threats seem highly plausible and inevitably attractive to cyber-criminals due to the hyper connectivity of a Smart Nation. Chaos and confusion could be caused if critical infrastructure

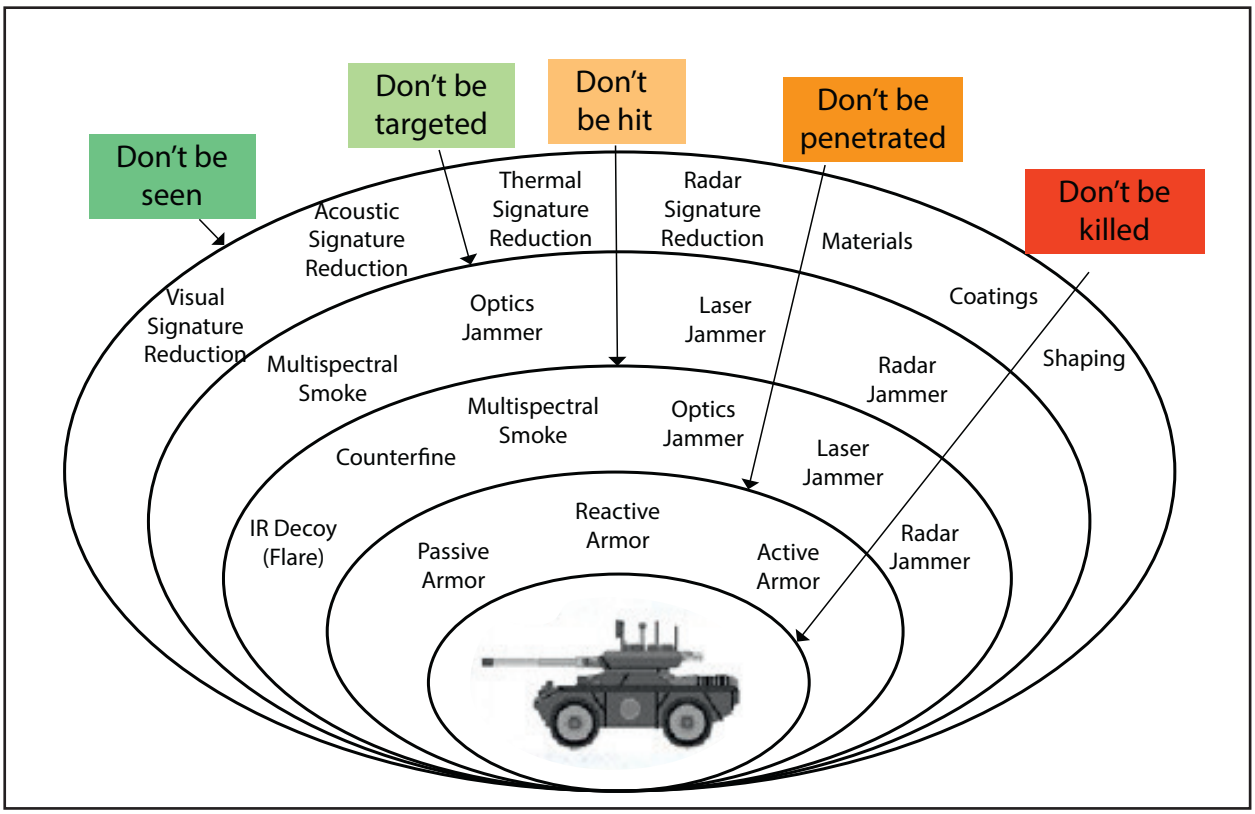


Figure 4: The Survivability Onion.[32]

and systems were to fall into the wrong hands, and spoof messages and transmissions were sent out.[33]

DEFENDING THE 'SMART' BATTLEFIELD

In recognising the threat of cyber attacks to its networks and systems, the SAF had established the Cyber Defence Operations Hub (CDOH) in 2013 to step up its cyber defence capabilities. Defence Minister Dr Ng Eng Hen had also announced that in enhancing cyber defence, the SAF will employ more artificial intelligence and big data analytics to detect and respond to cyber threats. The SAF will also build greater security into software design and network infrastructure to make them more resilient and resistant to cyber attacks. In parallel, cyber engineers and researchers from Defence Science Technology Agency (DSTA) and Defence Science Organisation (DSO) are working on advanced cyber defence solutions for MINDEF and the SAF. They aim to secure its networks, respond to cyber attacks and to safeguard its classified information and systems.[32]

In Singapore's bid to create the Smart Nation, various initiatives have been put in place to defend Singapore's 'Cyber' domain. CSA was set up in 2015 to co-ordinate the country's national efforts in cyber security. The Singapore Government has also embarked on a comprehensive blueprint that maps out Singapore's long-term approach towards securing its cyber space against incursions and to grow the ICT sector locally. Launching the national cyber security strategy at the opening of the first Singapore International Cyber Week in October 2016, Prime Minister Lee recognised that cyber security is 'an issue of national importance' as the country becomes more connected in its mission to become a Smart Nation.[34] One key prong of the strategy is directing more funds into defence against attacks. Mr Lee announced that about 8 per cent of the ICT budget will be set aside for cyber security spending, up from about 5 per cent before. The new proportion is similar to what other countries spend—Israel stipulates that 8 per cent of its total government IT budget must go to cyber

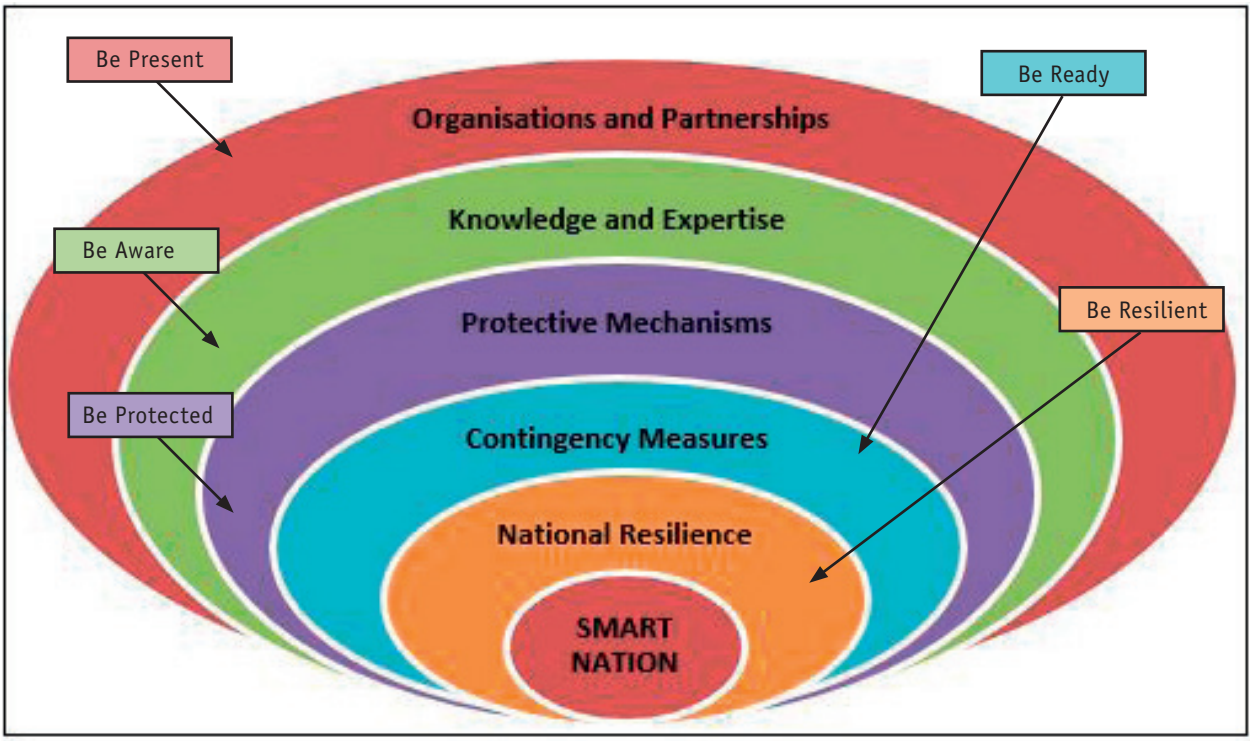


Figure 5: Adapting the Survivability Onion to Defending the Smart Nation

security, while South Korea channels as much as 10 per cent.[35]

So what more can be done to defend a Smart Nation? It is imperative to note that there never will be a 'one size fits all' solution, thus it is important to consider all possible options together. In his lecture on staying alive in the 21st Century, Dr Wilkes uses the Survivability Onion to demonstrate how risks and threats can be mitigated using a layered approach. Thus, I have adapted the Survivability Onion to protect against all levels of threats through a layered approach (See *Figures 4* and *5*).[36] I would be looking at five layers of defence to mitigate against any potential threats. They are essentially to be 'Present', 'Aware', 'Protected', 'Ready' and 'Resilient'. For the first layer, the Cyber Security Agency is currently already being set up in a whole of government approach as earlier mentioned. In terms of partnership, Singapore is looking to partner with other ASEAN member states and has been deploying 'cyber diplomacy' by building alliances with other countries, both to swop expertise, such as the latest in attack methods, and to regularly exercise and test its defences.[37] These measures ensure that Singapore is ever-present in all aspects of defending our Smart Nation. Next, I would be delving further into the other four layers of Knowledge & Partnerships, Protective Mechanisms, Contingency Measures and National Resilience.

BE AWARE – KNOWLEDGE AND EXPERTISE

Cultivate Cyber Security Experts

At the core of any cyber security initiative would be the need to build up a core of cyber security experts. It has been predicted that the demand for cyber security expertise will continue to increase. Currently, Singapore's educational institutes are starting programmes and initiatives to attract more talents for the cyber security workforce. The National University of Singapore and the Singapore Institute of Technology are starting undergraduate degree programmes in Information Security. The Nanyang Technological University and the Singapore Management University already have pre-existing cyber specialisation courses and modules while the Singapore University of Technology and Design has plans for a Master's degree in Cyber Security in future.[38] However, with the dire shortage of Cyber Security professionals worldwide, Singapore could consider tapping national servicemen with cyber security skills and knowledge.[39] With the announcement that pre-enlistees would be able to choose from 33 vocations across the SAF, police and civil defence in 2017, cyber security could be added as one of the preferred vocations that pre-enlistees could choose from.[40] Additionally, we could also consider dual vocations for National Servicemen who are already cyber security professionals.

Cyber Security Knowledge

It is not enough to have a group of experts in cyber security as cybersecurity is everyone's business and, a Smart Nation can only be as strong as its weakest link. It is therefore important for cyber security to be taught and shared with the different demographics of people in Singapore. A group that should not be missed would be new citizens, permanent residents as well as foreign workers in Singapore. A case in point would be the five foreign domestic helpers working in Singapore who were radicalised through social media. Thus, the introduction of the security course for all maids intending to work in Singapore is a welcome move. As terrorism has been increasing through the spread of social media and even women and children could be influenced, the launch of the SGSecure

So what more can be done to defend a Smart Nation? It is imperative to note that there never will be a 'one size fits all' solution, thus it is important to consider all possible options together.

programme in 2016 to rally more Singaporeans, foster resilience and prepare them to handle crises in the face of the looming terror threat is an important platform to share and impart cyber security knowledge.[41]

Figure 6: Circular addressing queries over new Net access rules.[42]

BE PROTECTED – PROTECTIVE MECHANISMS

Segregating Secure E-Mail from Internet Systems

There is a need for protective safeguards. One would be to protect secure e-mail systems by segregating them from the internet system. This measure, while inconvenient to users, could guard against cyber attacks over the internet that is possible when the systems are interconnected. Surfing separation will prevent attackers from using the Internet to plant malware to access Government computers or worse, an interconnected Smart Nation. Currently, this practice has already been implemented in the Ministry of Home Affairs (MHA) and MINDEF. However, the IDA has announced that it would be implementing this measure for all public servants come June 2017.[43] Separately, a circular (*Figure 6*) was sent out to address queries over the new Net access rules. It branded claims that the Government is cutting off the Internet for civil servants as a 'myth'. Dr Vivian Balakrishnan, then Minister-in-Charge of the Smart Nation Initiative, has reinforced that cyber security is essential if Singapore is to become a smart nation. Dr Balakrishnan said: "You can't afford a breach of privacy. So, the way I look at it, cyber security is the flip side of the coin of being a Smart Nation."[44]

First Responders

Next, first responder teams would need to be formed. An example is found in local power company Singapore Power which has a 'multi-faceted' approach to defending, detecting, responding and recovering from cyber attacks in place. A Singapore Power spokesperson has stated that there is a dedicated team on the lookout for 'unusual activities' on the grid around the clock. The company also hires external companies to conduct tests on its systems. "Our measures are tested and evaluated on a regular basis internally and also by professionals who perform audits and tests to ensure that our systems and procedures remain relevant and robust," the spokesperson said.[45] The company's comments come after a Western Ukraine power company Prykarpattyaoblenergo suffered an outage on 23rd Dec 2015, causing 700,000 people and half the homes in the Ivano-Frankivsk region in Ukraine to be without electricity for several hours.[46] To enhance Singapore's overall response to any cyber emergency, teams from

various companies could partner with the National Cyber Incident Response Teams (NCIRT) that are part of the national cyber response plan to enable a nationwide response.[47]

Cyber Security Range

In the military, wargaming is rudimentary in developing nascent operation concepts and processes, since they can be clinically tested without massive resources, as compared to the actual manoeuvring of forces. One possible cyber security measure and implementation is in developing a Cyber Range / Simulation System to enable the development and testing of cyber tools, best practices, policies for robustness in core system architecture. An example of such a facility is the National Cyber Range that was developed by the US Department of Defense in 2012 to allow co-operation with other US government agencies, and potentially non-US government partners to rapidly create numerous models of network. This was intended to enable the military and others to simulate cyber space operations and test new technologies and capabilities, promoting collaboration and critical info sharing, in support of a 'whole of nation' effort.[48]

BE READY – CONTINGENCY MEASURES

Ensuring Redundancy

Network Redundancy is an industry best practice to prevent critical network failure and improve stability. For example, if a point-of-failure occurs within the network infrastructure, the network redundancy will redirect data traffic to maintain a functional network and prevent widespread interruption of service. There are many different tools and hardware available to help create a redundant network. Hardware that has 'hot-swappable' components is especially helpful, as the network can be kept online while replacing failed components. Redundant hardware, such as battery backup systems, extra routers, switches and servers are also essential in the event of power failures or complete failure of essential devices. Beyond hardware, there are also protocols and software programmes that can maintain a stable network by autonomously detecting, addressing and alerting technicians of problems.[49]

Scenario and Contingency Planning

It is important to prepare for the worst and therefore it is vital to threat model all sorts of scenarios. The traditional scenario planning methodology, pioneered by Royal Dutch Shell, emphasises that scenarios are not intended to present definitive predictions about the future. Rather, scenarios help to articulate the risks and opportunities present in a range of plausible futures and serve as a discussion tool to stimulate debate about strategies to shape the future. Scenario planning was first introduced into MINDEF in the late 1980s and has since been approved by the government as a tool for long-term policy and strategic development.[50] Currently, the Singapore Government produces a set of National Scenarios every three to five years to spark discussion and fresh thinking about issues related to Singapore's future. The National Scenarios are complemented by Focused Scenarios, which are in-depth studies into specific topics, such as climate change or new media.[51] However, it is now critical to also add 'what if' scenarios for cyberattacks.

Table Top Exercise

Once the different contingency plans have been formulated, table top exercises can help to test the theoretical responses during an emergency and are important for reviewing plans without the need to

exhaust huge resource. In 2016, the CSA mounted its first multi-sector exercise, Exercise Cyber Star. The exercise comprises a series of scenario planning sessions, workshops and table-top discussions focusing on cyber incident management processes. The final exercise brought together over 100 participants, comprising sector leads and Critical Information Infrastructure owners from four sectors, namely Banking and Finance, Government, Energy and Infocomm. The exercise scenario covered different types of cyber attacks including web defacement, wide-spread data exfiltration malware infections, large-scale DDoS attacks and cyber physical attack.[52] However, besides the CSA, more agencies should partake in such exercises so as to keep their response plans warm and to establish key linkages.

It is not enough to have a group of experts in cyber security as cybersecurity is everyone's business and, a Smart Nation can only be as strong as its weakest link.

BE RESILIENT – NATIONAL RESILIENCY

Psychological Defence

Apart from building in multiple layers of failsafe and redundancy, the government will need to promote national resilience so that when technical malfunctions do strike, the country can swiftly bounce back and return to normalcy. Rather than aim for a perfect system that never fails, this might indeed be a more realistic approach.[53] The larger dangers arising from cyber attacks are public fear, panic and the corrosion of public trust in the things we often take for granted as being secure and reliable, such as public utilities, cloud computing and electronic transactions. In the wake of a cyber attack, our critical infrastructure and systemic response must be resilient, enabling our society to bounce back so that normalcy is restored without undue delay and unnecessary detriment. Rather than the security breach itself, much damage flows from an inadequate response to it.[54] Equipping the community with the knowledge and skills of basic and psychological first aid has another less overt benefit: it empowers people. It is a foil against that debilitating feeling of helplessness that may follow a catastrophe, and strengthens resilience that comes from that sense of preparedness in the face of unpredictable threats.[55] Thus, as part of Total Defence, the SGSecure movement is an important platform to continue to involve every Singaporean in playing a part, individually and collectively, to build a strong, secure and cohesive nation.

Psychological Preparation

There is a need for psychological preparedness to fight against terror threats. It has been opined that (1) Singaporeans may not be able to react with resilience and unity in the event of a terror attack due to the peace and security they experience daily; (2) the psychological impact of an attack may be overlooked as it may not be as obvious as physical impacts. Therefore, Singaporeans must be trained to deal with unpredictable events like terror attacks and help one another. Citizens and businesses need to learn how to respond to cyber security emergencies, preparing for cyber drills as we do in fire drills. For example, if our computers or mobile devices are taken over by ransomware, will we have backup plans or will we panic? Many countries—from Singapore to Estonia to Zambia—conduct cyber drills, which see government agencies and key businesses planning responses to cyber attacks. But such attacks would also affect thousands of citizens and small businesses, destroying their work or personal data, or disabling communication for days or weeks. They, too, need to be brought into this ecosystem of preparation.[56]

Apart from building in multiple layers of failsafe and redundancy, the government will need to promote national resilience so that when technical malfunctions do strike, the country can swiftly bounce back and return to normalcy.

CONCLUSION

Singapore's bid to become a Smart Nation is a journey that can provide many opportunities and benefits for the Singapore population. However, it is one that is also fraught with challenges. With the possibility that the networks and connectivity in the Smart Nation become a CoG and an acute vulnerability, it is important that we put in measures to counter the threat of cyber attacks which are becoming a norm. Just like the common catchphrase used to portray the existential threat of terrorism, 'a matter of when, not if,' it is crucial that a layered defence is taken against cyber attacks.[57] Thus, this essay has recommended adapting from the survivability onion to look at a layered defence to mitigate any potential threats faced and to ultimately make this Smart Nation 'Secure'.

ENDNOTES

1. National Research Council, Computers at Risk, (*National Academy Press*: Washington DC, 1991).
2. Balakrishnan, Anita "The hospital held hostage by hackers," *CNBC*, 16 February 2016, http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html
3. Skinner, Curtis "Los Angeles hospital paid hackers $17,000 ransom in bitcoins," *Reuters*, 18 February 2016, http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VR085
4. Kwang, Kevin, "Singapore can't be a Smart Nation if systems are vulnerable: CSA chief," *Channel Newsasia*, 9 June 2016, http://www.channelnewsasia.com/news/singapore/singapore-can-t-be-a/2858650.html
5 Tham, Irene "StarHub: Cyber-attacks that caused broadband outages came from customers' infected machines," *The Straits Times*, 26 October 2016, http://www.straitstimes.com/tech/starhub-cyber-attacks-that-caused-broadband-outages-came-from-customers-infected-machines
6. Au-Yong, Rachel, "Technology will also help Singapore to keep pace with world's top cities," *The Straits Times*, 25 November 2014, http://www.straitstimes.com/singapore/vision-of-a-smart-nation-is-to-make-life-better-pm-lee
7. Tegos, Micheal "IDA wants to make Singapore a Smart Nation. Here's what you need to know," *Tech In Asia*, 22 April 2015, https://www.techinasia.com/singapore-smart-nation-2015
8. Loke Kok Fai, "Singapore needs to stay ahead while pursuing Smart Nation vision: Vivian Balakrishnan," *Channel NewsAsia*, 12 April 2016, http://www.channelnewsasia.com/news/singapore/singapore-needs-to-stay/2688112.html
9. SPRING Singapore, "Setting the standard worldwide: intelligent city, Smart Nation," *Enterprise Singapore*, 3 August 2015, http://www.spring.gov.sg/Inspiring-Success/Enterprise-Stories/Pages/Setting-the-standard-worldwide-intelligent-city-Smart-Nation.aspx
10. Lui Tuck Yew, "Speech by Second Minister for Defence Mr Lui Tuck Yew at the MINDEF Pride Day 2015 Award Presentation Ceremony at Singapore University of Technology & Design," *MINDEF*, 2 September 2015, http://www.mindef.gov.sg/content/imindef/press_room/official_releases/sp/2015/02sep15_speech.html
11. Scales, Robert "Clausewitz and World War IV," *Armed Forces Journal*, 1 July 2006, http://armedforcesjournal.com/clausewitz-and-world-war-iv/
12. *TTW Asia*, "Innovation Driven Initiatives pave the way for Singapore's Smart Nation Vision", 27 April 2015, http://www.ttwasia.com/news/article/innovation-driven-initiatives-pave-way-singapores-smart-nation-vision/

13. Evans, Michael "Centre of Gravity Analysis in Joint Military Planning and Design: Implications and Recommendations for the Australian Defence Force," Security Challenges, Vol. 8, No. 2 (*Winter*, 2012): 81-104, http://www.regionalsecurity.org.au/Resources/Files/vol8no2Evans.pdf

14. Echevarria, Antulio J. II "Clausewitz's Center of Gravity: Changing our Warfighting Doctrine – Again!", *Clausewitz*, September 2002, http://www.clausewitz.com/readings/Echevarria/gravity.pdf

15. Laasme, Haly, "The role of Estonia is developing NATO's Cyber Strategy," *Cicero Foundation*, December 2012,http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf

16. Mills, John R. "The Key Terrain of Cyber," *Georgetown Journal of International Affairs*, 23 March 2013, http://journal.georgetown.edu/wp-content/uploads/2015/07/gj12712_Mills-CYBER-2012.pdf

17. Boyd, Robert "Secure Technology, Centers of Gravity and Homeland Security," *TinMore Institute*, December 2014.

18. Greathouse, Craig "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" Cyberspace and International Relations, *Springer-Verlag Berlin Heidelberg*, 2014.

19. ME5 Ho Wei Seng, Alan, "Cyber Attacks and the roles the military can play to support the National Cyber Security Efforts," *POINTER*, Vol. 42. No.3 (2016).

20. Tan Teck Boon, "Building a Smart Nation: A Nuanced Understanding of Hyper-Connected Singapore," *International Policy Digest*, 26 August 2015, http://intpolicydigest.org/2015/08/26/building-a-smart-nation-a-nuanced-understanding-of-hyper-connected-singapore/

21.http://www.tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply

22. Tan Teck Boon, "Building a Smart Nation: A Nuanced Understanding of Hyper-Connected Singapore," *International Policy Digest*, 26 August 2015, http://intpolicydigest.org/2015/08/26/building-a-smart-nation-a-nuanced-understanding-of-hyper-connected-singapore/

23. Walters, Riley, "Cyber Attacks on U.S. Companies in 2014," *The Heritage Foundation*, 27 October 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

24. Eilperin, Juliet and Entous, Adam, "Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say," *The Washington Post*, 30 December 2016, https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html

25. *BBC*, "Ukraine power cut 'was cyber-attack'," 11 January 2017, http://www.bbc.com/news/technology-38573074

26. Tham, Irene, "StarHub outage: Experts sound alarm on attacks by 'smart' devices," *The Straits Times*, 27 October 2016, http://www.straitstimes.com/tech/experts-sound-alarm-on-attacks-by-smart-devices

27. Bellinger, Lee, "Cyber attacks. Impacting everything.", *Independent Living News*, https://independentlivingnews.com/2015/01/21/202478-cyber-attacks-impacting-everything-from-the-national-grid-to-pacemakers-yet-the-government-remains-obsessed-with-climate-change/

28. Tham, Irene, "StarHub outage: Experts sound alarm on attacks by 'smart' devices," *The Straits Times*, 27 October 2016, http://www.straitstimes.com/tech/experts-sound-alarm-on-attacks-by-smart-devices

29. Paganini, Pierluigi, "ICS-CERT Surge In attacks against Energy Industry," *Security Affairs*, 2 July 2013, http://securityaffairs.co/wordpress/15820/security/ics-cert-surge-in-attacks-against-energy-industry.html

30. Perlroth, Nicole, "Traffic Hacking: Caution Light Is On," *New York Times*, 10 June 2015, http://bits.blogs.nytimes.com/2015/06/10/traffic-hacking-caution-light-is-on/?_r=0

31. Chan Yeng Kit, "Speech by Mr Chan Yeng Kit, Permanent Secretary (Defence), at Cyber Defenders Discovery Camp Awards Ceremony 2016," *MINDEF*, 6 June 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/06jun16_speech.html

32. Wilkes, David, "The survivability onion: how to stay alive in the 21st century," *Yorkshire Philosophical Society*, 2007,

https://www.ypsyork.org/events/the-survivability-onion-how-to-stay-alive-in-the-21st-century/

33. Chan Yeng Kit, "Speech by Mr Chan Yeng Kit, Permanent Secretary (Defence), at Cyber Defenders Discovery Camp Awards Ceremony 2016," *MINDEF*, 6 June 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/06jun16_speech.html

34. Tham, Irene, "Singapore cyber security strategy launched, half of public agencies separate Web surfing from work computers," *The Strait Times*, 10 October 2016, http://www.straitstimes.com/singapore/singapore-cyber-security-strategy-launched-half-of-public-agencies-separate-web-surfing

35. Tham, Irene, "Singapore rolls out high-level cyber security strategy," *The Straits Times*, 11 October 2016, http://www.straitstimes.com/singapore/spore-rolls-out-high-level-cyber-security-strategy

36. Ibid.

37. Lim Yan Liang, "Singapore's weapon: cyber diplomacy," *The Straits Times*, 23 October 2016, http://www.straitstimes.com/singapore/spores-weapon-cyber-diplomacy

38. Chan Yeng Kit, "Speech by Mr Chan Yeng Kit, Permanent Secretary (Defence), at Cyber Defenders Discovery Camp Awards Ceremony 2016," *MINDEF*, 6 June 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/06jun16_speech.html

39. Jayakumar, Shashi and Benjamin Ang. "Smart Nation, but will we be secure?", *The Straits Times*, 14 October 2016, http://www.straitstimes.com/opinion/smart-nation-but-will-we-be-secure

40. Koh, Fabian, "NS pre-enlistees can pick from 33 vocations," *The Straits Times*, 9 September 2016, http://www.straitstimes.com/singapore/ns-pre-enlistees-can-pick-from-33-vocations

41. Royston Sim, "SG Secure to equip people for crises," *The Straits Times*, 19 March 2016, http://www.straitstimes.com/singapore/sg-secure-to-equip-people-for-crises

42. *Channel NewsAsia*, "Govt's move is not to cut off Internet access for public servants: Vivian Balakrishnan," 10 June 2016, http://www.channelnewsasia.com/news/singapore/govt-s-move-is-not-to-cut/2861356.html

43. *Channel NewsAsia*, "No Internet access for public officers' work computers by next June," 8 June 2016, http://www.channelnewsasia.com/news/singapore/no-internet-access-for/2854528.html

44. *Software Defines Everything*, "海外分行的規劃實務", September 8 2016, https://vmshare.blogspot.com/2016/?view=classic

45. *Channel NewsAsia*, "Measures to fend off cyber attacks tested regularly: Singapore Power," 6 January 2016, http://www.channelnewsasia.com/news/singapore/measures-to-fend-off/2402694.html

46. Ibid.

47. *Cyber Security Agency of Singapore*, "Singapore's Cybersecurity Strategy," 2016, https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

48. ME5 Ho Wei Seng, Alan, "Cyber Attacks and the roles the military can play to support the National Cyber Security Efforts," *POINTER*, Vol.42. No.3 (2016).

49. Melancon, Joe "Network Redundancy," *Smart City Networks*, 10 March 2015, https://www.smartcitynetworks.com/network-redundancy/

50. *Public Service Division*, "Conversations for the Future," Singapore's Experiences with Strategic Planning (1988–2011), 2011.

51. *Centre for Strategic Futures and Civil Service College*, "Fore Sight – A Glossary."

52. *Cyber Security Agency of Singapore*, "CSA marks operational milestone with Exercise Cyber Star," 22 March 2016, https://www.csa.gov.sg/news/press-releases/exercise-cyber-star

53. Tan Teck Boon, "Building a Smart Nation: A Nuanced Understanding of Hyper-Connected Singapore," *International Policy Digest*, 26 August 2015, http://intpolicydigest.org/2015/08/26/building-a-smart-nation-a-nuanced-understanding-of-hyper-connected-singapore/

54. Tan, Eugene "Multi-stakeholder approach needed to tackle cyberthreats," *Today Online*, 10 October 2016, http://www.todayonline.com/singapore/multi-stakeholder-approach-needed-tackle-cyberthreats

55. Chong Siow Ann, "After the terror, winning the psychological war," *The Straits Times*, 8 October 2016, http://www.straitstimes.com/opinion/after-the-terror-winning-the-psychological-war

56. Jayakumar, Shashi and Ang, Benjamin, "Smart Nation, but will we be secure?", *The Straits Times*, October 14, 2016, http://www.straitstimes.com/opinion/smart-nation-but-will-we-be-secure

57. *Today Online*, "Attack on Singapore a matter of when, not if, says Shanmugam," 23 March 2016, http://www.todayonline.com/singapore/unless-we-turn-city-prison-not-possible-counter-every-terror-attack-shanmugam

ME6 Calvin Seah Ser Thong is currently on secondment to the Land Transport Authority's Rail Asset, Operations and Maintenance Group. He is an Army Engineer by vocation and was previously a Section Head in HQ Maintenance and Engineering Support. ME6 Seah holds a Bachelors of Engineering in Mechanical & Production Engineering from the Nanyang Technological University (NTU), a Masters of Science in Industrial and Systems Engineering from the National University of Singapore (NUS) and a Masters of Science in Defence Technology and Systems from NUS obtained under the SAF Postgraduate Award. He also attained a Masters of Science in Human Capital Management from NTU under the SAF-NTU Continuing Education Masters Programme and was placed on the Nanyang Business School's Dean's List. For this essay, ME6 Seah was awarded the Second Prize at the 2016/2017 CDF Essay Competition.

HYBRID WARFARE – A LOW-COST, HIGH-RETURNS THREAT TO SINGAPORE AS A MARITIME NATION

by **MAJ Bertram Ang Chun Hou**

Abstract:

The advent of hybrid warfare has raised concerns for Singapore with the potential challenges that it may bring. Being a nation surrounded by water on all sides with no natural resources, maritime trading has not only become a way to maintain sustenance, but a key contributor to Singapore's economy. An attack on Singapore's maritime sector would not only affect the way of life, but undermine the shipping and erode confidence in Singapore as a transhipment hub. While the SAF is already well-prepared against a conventional threat, a hybrid threat could inflict equal or even more damage than any conventional means and, at a lower cost to the adversary. This essay discusses the vulnerabilities in Singapore's maritime domain, and how an aggressor could exploit this to their gain through hybrid means, evading the SAF's conventional defence methods. The rationale behind a potential aggressor attacking Singapore through the maritime domain is also discussed, providing examples as to how a sabotage could affect the populace in Singapore. Various hybrid methods were also discussed while explaining the ineffectiveness of responding through conventional means to a hybrid threat. Lastly, the author provides recommendations on how the SAF can augment the Republic of Singapore Navy (RSN) to better combat a hybrid threat.

Keywords: Hybrid Threat; Maritime Industry; Economic Strangulation; Social Stability; Information Warfare; Whole-of-Government

INTRODUCTION

The term 'hybrid warfare' is a relatively recent term that was coined during the 2006 Israel-Hezbollah War, where the Hezbollah was able to effectively combine both guerrilla-type tactics as well as conventional warfare in the form of rocket and anti-ship strikes on their Israeli adversaries. More recently, the appearance of masked and unmarked 'little green men' in the Crimean region, as well as the ISIS campaign in Syria and Iraq, have refuelled discussion about hybrid warfare, what it actually looks like in practice, and its implications for the modern battlefield. Indeed, while some commentators believe hybrid warfare to be illustrative of modern warfare, others claim that the term causes confusion instead of being representative of reality.[1]

However, despite the wide ranging debate about what hybrid warfare is and what it entails, there is little conversation of it in Singapore's context. The discussion below will seek to explore why a potential aggressor may seek to utilise hybrid warfare, and how it may go about doing so. The concept of hybrid

warfare and its potential to enhance the ability of an aggressor to achieve broader strategic objectives will be explored, with examples used to substantiate the hypothetical tactics that may be employed.

First, a working definition of hybrid warfare as it is understood and practised in the current context will be proposed. Thereafter, Singapore's particular strategic vulnerabilities in the maritime domain will be discussed, and in particular, how the added dimension of hybrid warfare in the maritime domain represents a low-cost, high-return strategy that a hypothetical aggressor may seek to utilise. This will also highlight the possibility of an aggressor circumventing Singapore's relatively significant conventional capabilities. Finally, several means to meet the hybrid challenge will be recommended.

DEFINING THE NATURE OF HYBRID WARFARE

Commentators such as Dr. Frank Hoffman have described hybrid warfare as a 'blend of the lethality of state conflict with… irregular warfare', incorporating 'conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.'[2] These conflicts are also seen to be unconventional, high intensity, and protracted.[3] The United States (US) Army has similarly defined hybrid threats as 'the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects.'[4] Beyond this, the US Army Special Operations Command (USASOC) recognises that hybrid warfare is 'whole-of-government (WoG) in nature,' places a 'particular premium on unconventional warfare,' and involves 'all available diplomatic, informational, military, and economic means to destabilise an adversary.'[5]

While proponents of hybrid warfare argue that it represents a novel and significant development, detractors contend that it is simply not new. Some observe that the use of hybrid warfare as it is understood today extends back at least as far as the Peloponnesian War in the fifth century B.C.[6] Others opine that hybrid warfare is at best simply a 'subset of irregular warfare,' given that irregular warfare already highlights the use of a full range of military and other capacities.[7] Such critics note that the concept of hybridity is timeworn and that all wars are hybrid with only their specific features changing over time.[8]

Without wading too much into the debate, there are several evident characteristics of hybrid warfare that are relevant to the discussion. First, it encompasses an effective range of conventional and unconventional tactics, as a means to achieve political objectives that may include destabilising and fomenting disorder in a target state. A second key facet of hybrid warfare that distinguishes it from mere unconventional or irregular warfare is its deliberate ambiguity. This contributes to the possibility of an aggressor achieving its political and strategic goals without necessarily asserting a clear military victory through direct confrontation. A third distinguishing characteristic of hybrid warfare is its overriding emphasis that war cannot be confined to a specific dimension. Rather, conflict should always be viewed as a battle for influence, and can therefore be waged in any element, including the legal, diplomatic, economic and informational realms.

WHY THE MARITIME DOMAIN AS A SIGNIFICANT THREAT AXIS?

Maritime security (MARSEC), without even taking into consideration hybrid threats, has already been of concern for some time for maritime states such as Singapore. The attacks on the *USS Cole* in 2000, the

The Military Sealift Command fleet ocean tug USNS Catawba towing USS Cole after the bombing.

MV Limburg in 2002, and the 2008 Mumbai attacks represent just a few of the many incidents that have clearly demonstrated the devastating effects of unconventional attacks from the sea. In Singapore's context, this maritime vulnerability is two-fold. First, Singapore's status as a maritime nation and open nature as a port underscores the significance of its maritime sector while highlighting its high level of exposure to threats from the maritime axis. Worst-case scenarios envisage the use of ships as floating bombs or as delivery vehicles for explosive devices.[9] The security of Singapore's territorial waters and port limits must be managed despite the high volume of shipping that passes through, including the safety of its key installations (KINs) and infrastructure against potential unconventional attacks or sabotage. The fact that many such KINs, including petroleum and chemical industries, are located on the offshore Jurong Island makes the task more challenging given its close proximity to maritime traffic.

Second, beyond its shores, Singapore must be able to ensure its Sea Lines of Communication (SLOCs) remain constantly open to shipping. These SLOCs serve as key economic lifelines, given that the maritime industry in Singapore alone accounts for 7% of its Gross Domestic Product (GDP) and employs more than 170,000 people.[10] Beyond serving an economic purpose, these SLOCs are literally vital to Singapore's survival, providing its people with access to daily necessities such as food, oil and other material goods. The SLOCs can be seen as a key strategic vulnerability when the disproportionate ramifications of a single successful attack are considered, and when taking

Port of Singapore

into account that high-value shipping is a relatively soft target for such attacks. Furthermore, ensuring the SLOCs remain open is a daunting task, given their characteristics that render them vulnerable to disruption. For example, at the narrowest point in the Philips Channel located to the west of Singapore, the Malacca Strait is only 1.7 nautical miles wide, creating a natural chokepoint that can easily be exploited.[11] To the east, the SLOC extends through the hotly contested South China Sea up towards the Sea of Japan, making any maritime incident a potential flashpoint that could drastically affect seafaring, in turn resulting in negative implications for Singapore and its maritime economy.

THE ADDED DIMENSION OF HYBRID THREATS

> *"Be extremely subtle, even to the point of formlessness. Be extremely mysterious, even to the point of soundlessness. Thereby you can be the director of the opponent's fate."*
>
> *-Sun Tzu, The Art of War*[12]

While a potential adversary would have multiple avenues to consider how to best impose its will on Singapore, it is likely that it would elect to seek the means that best allow it to circumvent Singapore's conventional capabilities as a head to head military confrontation could prove overly costly to any aggressor. Furthermore, an adversary would strongly consider the maritime domain as its main attack axis given Singapore's existing maritime vulnerabilities, as already highlighted. Taking the above into account, a potential approach for a hybrid aggressor could be to conduct economic strangulation by weaving disparate unconventional actions into an extended and ambiguous period of tension at sea to deter and discourage trade and shipping. By ensuring its tactical actions remain unattributable, a potential aggressor could also potentially paralyse decision-making and bypass direct military confrontation.[13] The consequences of extended economic strangulation would undoubtedly affect the psychological will of the populace over time, undermining societal solidarity through an extended period of hardship.[14] Further supplementing these tactics with offensive information operations would also contribute towards sapping the national morale. On the whole, this represents a low-cost, high-return strategy against Singapore as a maritime nation that a potential adversary would strongly consider.

The task of defeating a hybrid threat cannot fall on the shoulders of the military alone, and must involve a WoG response that is co-ordinated and synergised.

There are several hypothetical possibilities open to the hybrid aggressor to achieve economic strangulation. For example, much like the unidentifiable 'little green men' in the Crimean region, unmarked Special Forces personnel operating under the guise of pirates or hijackers on fast craft could harass specific merchant ships, either Singapore-flagged merchantmen, or simply those with vital shipments bound for Singapore. Such information on cargo and ship destinations is readily obtained, even from open sources including the satellite-based Automatic Identification System (AIS) and Long-Range Identification System (LRIT).[15] Given that piracy and hijacking attempts are not uncommon in the region, it would not be difficult to ensure that these actions remain unattributable. If necessary, the aggressor could also introduce an element of 'terrorism' by attacking vulnerable shipping along the SLOCs,

particularly at narrow chokepoints, with portable missile systems or rocket-propelled grenades.[16] Such tactics have been previously employed by Egyptian militants operating along the banks of the Suez Canal. The risk of transiting through the targeted areas, coupled with the increased costs, would adversely affect shipping confidence, inevitably resulting in the reduction of trade and a negative impact on Singapore's economy. There is certainly precedence—Lloyd's of London declared the Malacca Straits a high war-risk area in 2005 for insurance purposes due to multiple incidents of piracy and sea robbery, resulting in additional premiums on ships transiting in the area and increasing the cost of shipping.[17] The economic impact will also be exacerbated by the negative societal implications arising from the reduced availability of food, oil and daily necessities over an extended period of time.

While the idea of using naval blockades to literally starve a target state into submission is not original, the concept of exploiting unattributable and non-conventional actions to avoid potential international backlash and to paralyse the target state would be a novel and effective way of achieving the same strategic goal. As the Russian Chief of the General Staff, General Valeriy Gerasimov noted, "the role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[18]

An effective hybrid aggressor would also supplement the above with information warfare, which could be extremely effective in eroding social stability and the national will to fight. The importance of information warfare can be observed from the Israel-Hezbollah war, where the battle for 'perception dominance' was critical.[19] As observers noted, the incisive use of 'the camera and the computer [as] weapons of war' in information operations allowed Hezbollah to come out of the conflict stronger in ideological appeal.[20] Adversarial propaganda and information operations utilising selective reporting and the power of social networks, could be used to incite and exacerbate existing social unrest generated as a result of the scarcity of material goods, and even undermine the government by fomenting further population discontent with the deteriorating situation.

Beyond serving an economic purpose, these SLOCs are literally vital to Singapore's survival, providing its people with access to daily necessities such as food, oil and other material goods.

Even if a conventional military response were to be successfully mounted, a successful hybrid aggressor would be able to mitigate and counter these actions by exploiting constraints imposed on conventional armed forces like the SAF. This would include rules of engagement, political will, and norms of warfare.[21] As observers have noted, fishing vessels can serve as intelligence collecting vessels, acting as a potent tool to 'dominate the seascape without the risk of open conflict.'[22] This is because the destruction or harassment of these 'innocent' vessels by the target state would surely become the focus of propaganda that portrays it in an unflattering light, thereby causing it to lose the moral high ground.[23] In the hypothetical context above, the harassment of merchant shipping bound for Singapore could be conducted from similarly 'neutral' vessels that could then easily vanish among the multiple fishing fleets that ply the South China Sea and Straits of Malacca. If and when confronted, these same vessels can easily

turn the tables in the public sphere through the clever manipulation of information and imagery.

WHAT CAN BE DONE?

In terms of military preparation, military training should be revamped to take irregular and unconventional tactics into greater consideration. Given the ambiguity and versatility of hybrid threats, such training should be conducted to prepare the men and women of the SAF to be similarly adaptable. As observers note, there is a need to focus on the cognitive skills required to recognise, react and adapt to new situations, complemented by a greater emphasis placed on continual organisation learning and adaptation.[24] Soldiers, sailors and airmen must be ready and able to perform wartime roles in peacetime, and peacetime roles in wartime effectively, without being paralysed into inaction by the seeming dissonance. Crucially, the military must grasp the need to be media savvy in the new information age. They must not only know how to defend themselves and their actions, which will come under greater scrutiny especially in the online sphere, but be shrewd enough to use new media to their own advantage in tactical situations. If the camera and computer are no different from a rifle or missile as weapons of war, it is only prudent and logical that our personnel are similarly trained and equipped to use them effectively.

Since it is evident that one of Singapore's greatest strategic vulnerabilities lies in its exposure to maritime threats, the navy in particular must be well-equipped and sufficiently resourced. In the first place, the navy must not be inadvertently shackled by its own norms and rules. In practical terms, the naval vessels of today should be equipped with a spectrum of weapons and equipment that allows them to calibrate their responses out at sea. For example, the use of water cannons, which have been installed onboard the new *Independence*-class Littoral Mission Vessels (LMV), gives the navy expanded options for calibrated responses that may help it avoid accusations of disproportionate force when responding to 'peacetime' incidents.

RSN's Littoral Mission Vessel RSS Independence

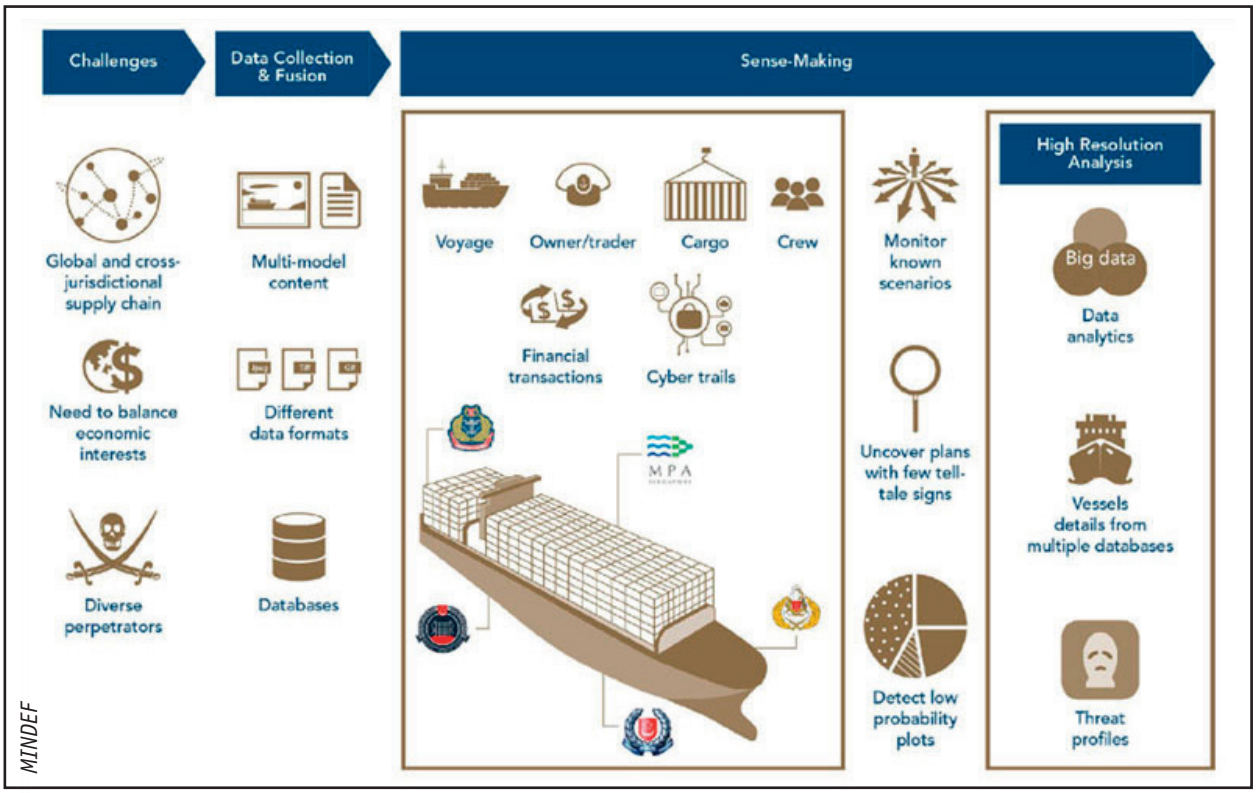
Crucially, the military must grasp the need to be media savvy in the new information age. They must not only know how to defend themselves and their actions, which will come under greater scrutiny especially in the online sphere, but be shrewd enough to use new media to their own advantage in tactical situations.

These responses must in turn be supported by a robust framework of Rules of Engagement (ROE), which should be expanded to deal with the widening spectrum of potential incidents that can occur. A robust ROE framework that caters for a wide range of incidents and responses will empower on-scene commanders with greater autonomy and enhance their ability to deal with irregular and unexpected threats in peacetime and troubled peace. At the same time, to close decision loops more expeditiously, shore-sea data networks must be enhanced and capitalised on to facilitate real-time updates and allow commanders on shore to better grasp the situation and react appropriately. The navy must therefore also be prepared to become an increasingly deployed one, with vessels that are able to put to sea at a moment's notice to react to incidents at sea.[25]

That being said, the navy must be able to take the initiative rather than merely being reactive. Beyond being prepared to go to sea, the idea of becoming increasingly deployed also connotes the need to have the 'legs' to be able to maintain a continuous presence. This is necessary if the navy wants to adopt a proactive posture through show-of-presence patrols and escorts in order to project a deterrent posture and prevent incidents from taking place, and to police the SLOCs over a protracted period of tension. When taking into account the navy's future manpower, resource and logistics constraints, it is imperative to leverage technology. In this instance, conventional naval vessels would need to be significantly augmented with unmanned surface vessels (USVs). This is not implausible—for example, the *Venus 16* unmanned surface craft was recently unveiled at the 2015 edition of Exercise Highcrest. Featuring in-built collision-avoidance protocols, it has already demonstrated its ability to autonomously conduct patrols.[26]

The task of defeating a hybrid threat cannot fall on the shoulders of the military alone, and must involve a WoG response that is co-ordinated and synergised. In this respect, Singapore has already taken steps to address its maritime vulnerabilities through implementing WoG measures such as the setting up of the Maritime Security Task Force (MSTF) in 2009 and the establishment of the Singapore Maritime Crisis Centre (SMCC) in 2011 to institute a synchronised approach to MARSEC. The SMCC in particular is able to build profiles of vessels based on data sharing with the rest of the shipping industry, thereafter conducting analysis to determine anomalous behaviour.[27] However, while such measures may be able to address single or short-term MARSEC threats, it would arguably be challenging to deal with a spectrum of maritime threats taking place over an extended duration of time, as part of a deliberate hybrid campaign to undermine the national will to fight.

Here, the concept of 'Total Defence' in peacetime will be useful, given that the development of societal resilience does not occur overnight. By focusing on building up social and psychological defence in peacetime, Singapore can create an emotional and psychological buffer for its populace that will play an important role in defending the national psyche and



Infographic on how Singapore's Maritime Security Task Force deal with challenges.

will against attacks, while simultaneously helping society withstand the stress of an extended duration of economic and material privation.

Furthermore, the WoG response must be complemented with offensive and defensive information campaigns. Offensive information campaigns should serve the purpose of penetrating the shroud of disinformation and exposing the enemy on multiple media platforms once they are identified. These campaigns must also be complemented by diplomatic initiatives to garner and exert international pressure on the aggressor to cease and desist. However, these offensive information campaigns are insufficient. Even if the perpetrators are identified, there must also be defensive information campaigns to sustain a spirit of resilience within the population, a quality that would undoubtedly be required to deal with the economic and social instability that comes with an extended period of uncertainty.

CONCLUSION

> *"Whether it be the intrusions of hackers, a major explosion at the World Trade Center, or a bombing attack by bin Laden, all of these greatly exceed the frequency band widths understood by the American military."*
>
> *-Qiao and Wang*
> *Unrestricted Warfare*[28]

With remarkable insight, Qiao and Wang, two Chinese colonels, predicted the World Trade Center attacks before they occurred. Much like General Gerasimov, Colonels Qiao and Wang argued that alternative, non-military methods of warfare could achieve the same effect of forcing states to give in to demands, thereby having similar or even greater destructive force than military warfare.[29]

They commented that given the American inability to contemplate non-traditional means of warfare, selecting non-military or non-direct concepts of operation would enable such attacks to succeed.[30]

It is not far-fetched to believe that potential adversaries would similarly choose to avoid a direct confrontation and opt instead for other forms of warfare to achieve the same strategic goals, exploiting Singapore's maritime strategic vulnerabilities while simultaneously avoiding its relatively significant conventional capabilities. It may be true that the term and practice of 'hybrid warfare' is merely an embellishment of a long-established way of conflict. However, the implications of alternative, unconventional and irregular means of warfare being coupled with modern day technologies and techniques are grave, and would be a formidable tool in the hands of an adversary, especially one seeking to avoid a direct confrontation. As such, while the SAF continues to hone its conventional edge, it must also be wary and cognisant of other means of warfare that seek to bypass its strengths while allowing an aggressor to achieve the same strategic goals at a much lower cost.

BIBLIOGRAPHY

Chee Hean, Teo. Speech given at the 30th Anniversary Gala Dinner of the Singapore Shipping Association, Singapore, September 25, 2015. Accessed January 1, 2016. http://www.mpa.gov.sg/sites/global_navigation/news_center/speeches/speeches_detail.page?filename=sp150925.xml

Coalson, Robert. "Top Russian General Lays Bare Putin's Plan for Ukraine." *The World Post,* (2014). http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html

Dr. Eng Hen, Ng. Speech given at the Committee of Supply Debate 2015, *MINDEF,* http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05mar15_speech.html#.VoZ6Qlmo0g4

Dr. Glenn, Russell W. "Thoughts on Hybrid Conflict". *Small Wars Journal* (2009). Accessed January 5, 2015, http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf

Dr. Latawski, Paul. "The Inherent Tensions in Military Doctrine". *Sandhurst Occasional Paper No.5* (2011). Accessed January 6, 2016. http://www.army.mod.uk/documents/general/RMAS_Occasional_Paper_5.pdf

Dr. Van Puyvelde, Damien. "Hybrid war—does it even exist?" *NATO Review*. Accessed December 31, 2015. http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

Eckstein, Megan. "U.S. Naval Commander in Europe: NATO Needs to Adapt to Russia's New Way of Hybrid Warfare." *USNI News*. October 6, 2015. http://news.usni.org/2015/10/06/u-s-naval-commander-in-europe-nato-needs-to-adapt-to-russias-new-way-of-hybrid-warfare

Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hoffman, Frank G. "Lessons from Lebanon: Hezbollah and Hybrid Wars." *Foreign Policy Research Institute*, August 2006. http://www.fpri.org/articles/2006/08/lessons-lebanon-hezbollah-and-hybrid-wars

Kalb, Malvin and Carol Saivetz. "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." *Research Paper Series, Joan Shorenstein Center on the Press, Politics and Public Policy*, February 2007. http://shorensteincenter.org/wp-content/uploads/2012/03/r29_kalb.pdf

James Kraska and Michael Monti. "The Law of Naval Warfare and China's Maritime Militia. *International Law Studies, U.S. Naval War College*, Vol 91, 2015. http://stockton.usnwc.edu/cgi/viewcontent.cgi?article=1406&context=ils

Liang, Qiao and Wang Xiangsui. Unrestricted Warfare: China's Master Plan to Destroy America. *Panama City: Pan American Publishing Company*, 2002.

LTC Lim, Nicholas. "Information Sharing to Enforce Security in the Maritime Domain." POINTER Supplement, The Information Fusion Centre: Challenges and Perspectives (2011): 3-10.

MAJ. Fleming, Brian P. "The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art". *School of Advanced Military Studies*. Accessed 2 January, 2016. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ada545789

Mansoor, Peter R. "Introduction: Hybrid Warfare in History."

In *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, edited by Williamson Murray and Peter R. Mansoor, 1- 17. *New York: Cambridge University Press*, 2012.

MINDEF. "Factsheet: Singapore Maritime Crisis Centre." Accessed January 1, 2016. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2015/nov/05nov15_nr/05nov15_fs1.html#.VoX-61mo0g5

Moller, Bjorn. *Piracy, maritime terrorism and naval strategy*. Copenhagen, *Denmark: Danish Institute for International Studies*, 2009. https://www.ciaonet.org/attachments/13744/uploads

Reuters. "Factbox – Malacca Strait is a strategic 'chokepoint,'" *Reuters*, March 4, 2010. Accessed 1 January, 2016. http://in.reuters.com/article/idINIndia-46652220100304

Spencer, Richard. "Suez Canal targeted as war in Sinai spreads." *The Telegraph*. November 17, 2013. http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/10454020/Suez-Canal-targeted-as-war-in-Sinai-spreads.html

Thomas, Bobby. "Malacca strait a 'war risk zone'? Lloyd's should review its assessment." *IDSS Commentaries* 57/2005. https://www.rsis.edu.sg/wp-content/uploads/2014/07/CO05057.pdf

U.S. Army. *Field Manual 3-0 Operations C-1*. Washington, DC: GPO, 2011.

U.S. Army Special Operations Command. "Counter-Unconventional Warfare White Paper". September 26 2014. Accessed December 31, 2015. https://info.publicintelligence.net/USASOC-CounterUnconventionalWarfare.pdf

Wong, Kelvin. "Singapore unveils Venus 16 unmanned surface vehicle." *IHS Jane's 360*. 4 November 2015. http://www.janes.com/article/55775/singapore-unveils-venus-16-unmanned-surface-vehicle

ENDNOTES

1. Dr. Damien Van Puyvelde, "Hybrid war—does it even exist?" *NATO Review* (2015), http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm
2. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (*Arlington, VA: Potomac Institute for Policy Studies*, 2007), 28-29. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
3. Ibid.
4. U.S. Army, *Field Manual 3-0 Operations C-1* (GPO, Washington, DC: February 2011), 1-5
5. U.S. Army Special Operations Command. "Counter-Unconventional Warfare White Paper" (2014): 3,https://info.publicintelligence.net/USASOC-CounterUnconventionalWarfare.pdf
6. Peter R. Mansoor, "Introduction: Hybrid Warfare in History," in Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, ed. Williamson Murray et al (*New York: Cambridge University Press*, 2012), 3.
7. Dr. Russell W. Glenn, "Thoughts on Hybrid Conflict". *Small Wars Journal* (2009), http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf
8. Dr. Paul Latawski, "The Inherent Tensions in Military Doctrine". *Sandhurst Occasional Paper No.5* (2011): 23, http://www.army.mod.uk/documents/general/RMAS_Occasional_Paper_5.pdf
9. Bjorn Moller, Piracy, maritime terrorism and naval strategy, (*Copenhagen, Denmark: Danish Institute for International Studies*, 2009), 23. https://www.ciaonet.org/attachments/13744/uploads
10. Teo Chee Hean, Speech given at the 30th Anniversary Gala Dinner of the Singapore Shipping Association, Singapore, September 25, 2015, http://www.mpa.gov.sg/sites/global_navigation/news_center/speeches/speeches_detail.page?filename=sp150925.xml
11. Reuters. "Factbox – Malacca Strait is a strategic 'chokepoint,'" *Reuters*, March 4, 2010, 2016, http://in.reuters.com/article/idINIndia-46652220100304
12. Sun Tzu. Sun Tzu on The Art of War, (*Allandale Online Publishing*, 2000),

    https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf
13. Megan Eckstein, "U.S. Naval Commander in Europe: NATO Needs to Adapt to Russia's New Way of Hybrid Warfare," *USNI News*, October 6, 2015, http://news.usni.org/2015/10/06/u-s-naval-commander-in-europe-nato-needs-to-adapt-to-russias-new-way-of-hybrid-warfare
14. Dr. Ng Eng Hen, Speech at the Committee

of Supply Debate 2015, *MINDEF* http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05mar15_speech.html#.VoZ6Qlmo0g4

15. LTC Nicholas Lim, "Information Sharing to Enforce Security in the Maritime Domain," POINTER Supplement The Information Fusion Centre: Challenges and Perspectives (2011) :7.

16 Richard Spencer, "Suez Canal targeted as war in Sinai spreads," *The Telegraph*, November 17, 2013, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/10454020/Suez-Canal-targeted-as-war-in-Sinai-spreads.html

17. Bobby Thomas, "Malacca strait a 'war risk zone'? Lloyd's should review its assessment," (*IDSS Commentaries* 57/2005).https://www.rsis.edu.sg/wp-content/uploads/2014/07/CO05057.pdf

18. Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *The World Post*, February 11, 2014, http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html

19. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (*Arlington, VA: Potomac Institute for Policy Studies*, 2007), 38. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

20. Malvin Kalb and Carol Saivetz, "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict," (*Research Paper Series, Joan Shorenstein Center on the Press, Politics and Public Policy*, February 2007), 4, http://shorensteincenter.org/wp-content/uploads/2012/03/r29_kalb.pdf

21. MAJ. Brian P. Fleming. "The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art" (Monograph, *School of Advanced Military Studies*, 2011), 33. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ada545789

22. James Kraska and Michael Monti, "The Law of Naval Warfare and China's Maritime Militia," (*International Law Studies, U.S. Naval War College*, Vol 91, 2015): 451,http://stockton.usnwc.edu/cgi/viewcontent.cgi?article=1406&context=ils

23. Ibid., 454,466.

24. Frank G. Hoffman, "Lessons from Lebanon: Hezbollah and Hybrid Wars," *Foreign Policy Research Institute*, August 2006, http://www.fpri.org/articles/2006/08/lessons-lebanon-hezbollah-and-hybrid-wars

25. Megan Eckstein, "U.S. Naval Commander in Europe: NATO Needs to Adapt to Russia's New Way of Hybrid Warfare," *USNI News*, October 6, 2015, http://news.usni.org/2015/10/06/u-s-naval-commander-in-europe-nato-needs-to-adapt-to-russias-new-way-of-hybrid-warfare

26. Kelvin Wong, "Singapore unveils Venus 16 unmanned surface vehicle," *IHS Jane's 360*, 4 November 2015, http://www.janes.com/article/55775/singapore-unveils-venus-16-unmanned-surface-vehicle

27. "Fact Sheet: Singapore Maritime Crisis Centre," *MINDEF*, accessed January 1, 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2015/nov/05nov15_nr/05nov15_fs1.html#.VoX-61mo0g5

28. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, (*Panama City: Pan American Publishing Company*, 2002).

29. Ibid., 96.

30. Ibid., 122.

MAJ Bertram Ang Chun Hou is currently enrolled in the United States Naval War College as an International Masters candidate in the Naval Staff College, and is also pursuing a graduate certificate in Ethics and Emerging Technology. He previously graduated from Stanford University with a Bachelor of Arts in Political Science and Economics, with interdisciplinary honours in International Security Studies. MAJ Ang is a Naval Combat Officer by vocation. He has served operational tours on board the missile corvettes and frigates, and was previously the Branch Head of the Strategic Futures Branch in Policy Office, MINDEF.

WINNING HEARTS THROUGH COMMUNICATION – A SOCIAL MEDIA ENGAGEMENT STRATEGY FOR THE MILITARY

by **MAJ(NS) Tan Kok Yew**

Abstract:

According to the author, with the high social media penetration rate in Singapore, it would be beneficial if a model to engage military personnel through the Social Media could be promulgated to guide commanders, human resource managers and communication practitioners. This essay will combine a military retention framework derived from civilian employee retention models and gaps in existing military employee retention frameworks, applying it to Social Media strategies to devise a Social Media engagement model to propose an enhancement to military employee retention in the SAF. The POWERS framework proposed, together with a pilot study with six respondents, would serve to provide the first step towards an effective employee retention model for the SAF.

Keywords: Social Media; Social Presence; Communication; Employee Retention; Organisation

INTRODUCTION – APPLYING CIVILIAN THEORIES IN THE MILITARY

> *"The art of communication is the language of leadership."*
>
> *- James C. Humes,*
> *Author and Former Presidential Speechwriter.*[1]

Conventionally, research on civilian employee retention theory has treated retention as an instance of motivated personal choice largely influenced by dispositions, attitudes and feelings.[2] Using these established norms, a military retention model (See *Figure 1*) based on distal predictors and proximal predictors were proposed by Capon, Chernyshenko and Stark in 2007 for the New Zealand military, revolving around these three main factors. After distillation, the distal predictors were classified as perceived organisational support; work-family conflict; dispositions; and (whether the job has) met expectations. The proximal predictors were community involvement; job involvement; organisational commitment; and work satisfaction. However, this model focused only on the intentions to remain in the military, as opposed to widely expounded models on intentions to leave.[3] Another research by Devi in 2009 emphasised that employee engagement is a 'two-way street' and elaborated that a key success in the modern globalised economy is the creation of a 'retention-rich organisation' that could attract, engage and build lasting loyalty among its most talented employees.[4] This further motivated the research to explore the means of introducing civilian or commercial employee engagement philosophies into the military, like the SAF, to create a 'retention-rich' military organisation.

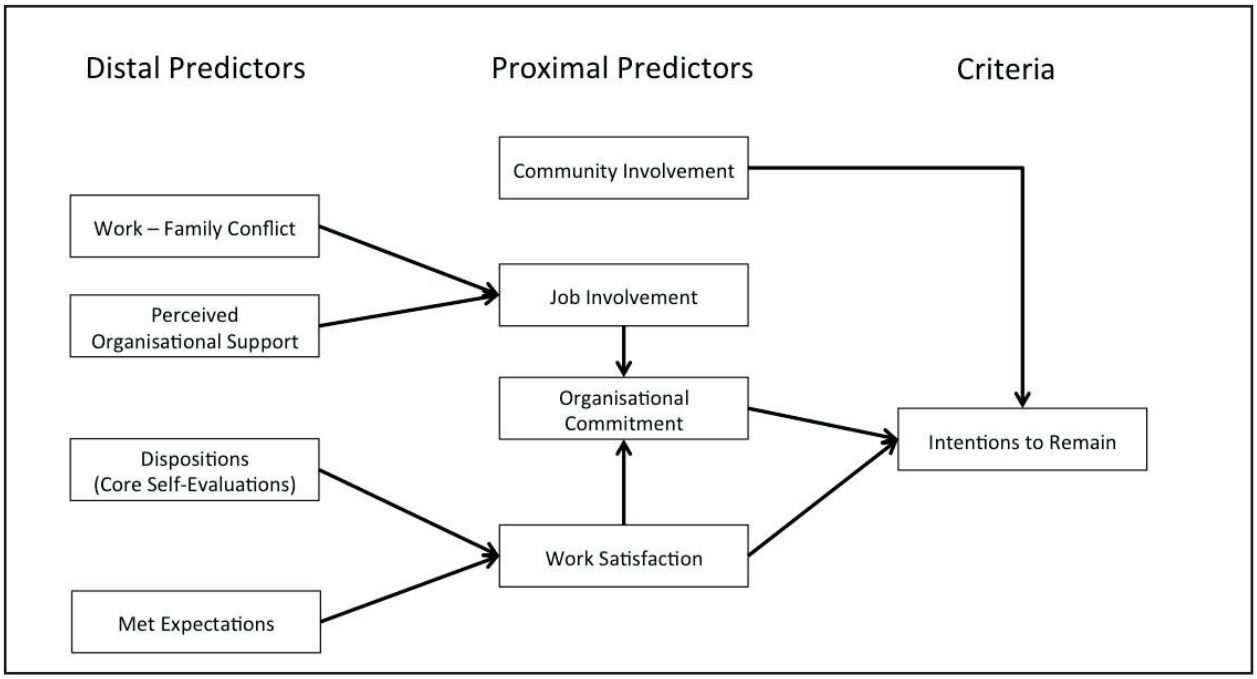


Figure 1: "Personal Choice" military retention model.[5]

With the high social media penetration rate in Singapore, it would be beneficial if a model to engage military personnel through the Social Media (SM) could be promulgated to guide commanders, human resource managers and communication practitioners.[6] This essay will combine a military retention framework derived from civilian employee retention models and gaps in existing military employee retention frameworks, applying it to SM strategies to devise a SM engagement model to propose an enhancement to military employee retention in the SAF. The POWERS framework proposed, together with a pilot study with six respondents, would serve to provide the first step towards an effective employee retention model for the SAF.

TO LEAVE OR NOT TO LEAVE – CAN POWERS SOLVE THE PROBLEM?

In the literature of employee turnover, Krueger opined that a certain number of military personnel leave the organisation as they are unable to cope with the strenuous physical requirements as military jobs are naturally physically and psychologically demanding.[7] Due to the nature of military training, there is a sizeable number of personnel turnover caused involuntarily and these cases should be discerned from the voluntary resignations. Sucharski and Rhoades proposed that the perceived supervisor and organisation support for employees play a major role in employee turnover rate.[8] This is especially distinct in large organisations like the military as opposed to small and medium enterprises where perceptions of supervisors and organisations might be grey, coupled with the characteristics of the Gen Y population who have dominated the industries.[9] Another research by Eisenburger *et al*. also inferred that leadership styles that precipitate sour relations between military leaders and lower ranking members are a major contributor to military turnover.[10] This adds on to the interest to ascertain how and what kind of relationship or perceived supervisor support affects military turnover or retention rate. Eisenberger *et al*. further suggested that superiors, to the extent that they are identified with the organisation, contribute

to perceived organisational support and, ultimately, to employee retention. [11] This is particular apparent to the military, where the commanders are the organisation's reach to its men (or employees) by hierarchy and structure. Commanders are hence the advocates for the organisation and will have to be strong believers in the organisation's visions, and be a supernode in communication.[12]

With the factors listed in the various retention models, it is important for this essay to then address some of the problems the SAF might face when communicating the value of serving in the military to its own people. The level of employee engagement by the organisation and its corresponding effect on employee retention is one of the key aspects to examine in this SM-dominated era when referring to communications with employees. Social Presence, which refers to the degree of salience of the other person in the communication interactions and the consequent salience of the interpersonal relationship, translates to how well the recipient feels the presence of the communicators, especially in this era when employee communication has moved on to SM platforms.[13] While the conventional military settings might not augur well with trend-setting user-generated environment in the SM, it is inevitable that the military has to venture towards where the hearts and minds are in order to strike the right chord.

Drawing reference from the communication research by Wright and Hinson on how new communications media are being used in public relations, it is evident that SM is becoming increasingly important for organisations and public service entities, including the military, in its employee engagement and community identity campaigns. [14] Relating back to the Personal Choice Military Retention Model (PCMRM) by Capon, Chernyshenko and Stark, SM can help to influence Perceived Organisational Support, Community Involvement (or identity) and Organisational Commitment, covering both distal and proximal predictors. As this essay would aim to design a SM communication framework for military employee engagement, the three predictors mentioned will be transferred over to the envisioned framework and explained in detail.

P	**erceived Organisational Support**	*Am I important to the organisation?*
O	**rganisational Commitment**	*How much do I love the organisation?*
W	**ork Satisfaction**	*How happy am I in the organisation?*
E	**ngagement**	*Do I feel like I am part of the organisation?*
R	**ealisation of Expectations**	*Is the organisation giving me what I want?*
S	**ocial Involvement**	*Is my organisation well regarded by the society?*

Figure 2: The POWERS Framework and the probing question for each element – Perceived organisational support, Organisational commitment, Work satisfaction, Engagement, Realisation of expectations, and Social involvement.

Combining the key factors from models across literature on employee retention and military employee turnover rates, a conceptual framework examining both push and pull factors is proposed, which would serve as a useful model for military commanders' reference. The proposed framework, POWERS (See *Figure 2*), is a distillation of key factors for employee retention in the military context, with consideration for its application in various platforms including SM.

Perceived Organisational Support, as highlighted earlier in the PCMRM, supposes that there are socio-emotional needs of employees that they try to meet while determining the organisation's readiness to reward additional work effort. These lead to the development of global beliefs concerning the extent to which the organisation values their contributions and cares for their well-being.[15] It is deduced that this is an important piece of the puzzle to allow military employees to still hold the belief that their presence are valued, and continue to stay engaged with their commitment.

Organisational Commitment was defined by Steers as 'the relative strength of an individual's identity with, and involvement in, a particular organisation.'[16] Organisational commitment was also further broken down into more assessable components like affective, normative and continuance.[17] This essay focuses on the affective aspect as there is sufficient empirical evidence to establish that affective organisational commitment is a good predictor for intention to remain in an organisation.[18]

Work Satisfaction speaks for itself and is closely correlated with organisational commitment. But many studies have found that work satisfaction is less strong an indicator in predicting retention.[19] Work satisfaction is defined as one's affective attachment to his/her work role.[20] And, Griffeth *et al.* premised that work satisfaction is the best predictor of intentions. Hence it is important to include this aspect as it would have a substantial effect on retention or turnover.[21] This is particularly important in the military, a civil service, without high remunerations, which would require a lot more intangible rewards like work satisfaction to fuel the passion and commitment.

With each element of the POWERS framework defined, we see the importance and relevance of drawing reference from civilian employee retention models and adding context based on the military setting and demographics of the target audience.

Engagement is the level at which the employees are being engaged at work. It could be along the lines of openness to feedback, meaning or purpose of job, or development of the employees. Sunil reviewed the motivation theories of employees and derived a framework identifying critical factors among the respective motivation theories and the implications for developing and implementing employee retention practices.[22] Within the list of critical factors, employees' development and feedback stood out as key pillars supporting the aspect of engagement. The working environment needs to provide a challenge or offer new learning opportunities for employees to feel engaged. This is apart from the prospects of advancement and development of individuals, which are expected of an organisation. Engagement, in terms of employees' development and feedback hence become an important element within the POWERS framework which the SAF could consider in its employee retention strategies. In communication, it is important to profile human-interest success stories

With the platform chosen, and a framework to adopt, the approach will be a reverse-engineer of a qualitative content analysis—using key words and a coding list to categorise the standing of a communication effort using the POWERS framework.

and provide channels for employees to interact with career planners so as to make career development and planning a two-way conversation.

Realisation of Expectations combines the essence of the Expectancy Theory, Vroom's Theory and Porter and Lawler's Extension as nicely summed up by Sunil.[23] 'The expectancy theory holds that people are motivated to behave in ways that produce desired combinations of expected outcomes', hence the realisation of employees' expectations would be important to produce the desired organisational outcome. [24] Extending the Vroom's Theory, Porter and Lawler developed a model, which attempted to identify the source of people's valences and expectancies, stating that employees should exhibit more effort when they believe they will receive their desired reward upon completion of task.[25] Relating to this research, the level of realisation for the individual's expectations would be a predictor of intentions as well. This is especially the case when there is a basis for comparison in a job outside the military. Whether or not SAF and its commanders can gather, effectively, the expectations of the employees, and match them, would very much determine how long an employee would remain in service. While instant gratification might not be possible in a hierarchical organisation like the military, other forms of rewards can be explored instead of tangible ones like promotion and pay rise.

Social Involvement as a factor for employee retention is crucial in the military due to the nature of the job being a civil service, and remuneration which might not match up to what the commercial world could offer. This would mean that society's regard for the military should instil a strong sense of purpose and pride in the military employees for them to continue their service. Increasingly, it can be

Figure 3: SM penetration in Singapore with FB amongst the top 3.[26]

seen that the SAF and MINDEF have been enhancing public awareness of its missions and role in Singapore's defence through community relations efforts and public engagement activities. These are avenues which the servicemen could draw reference to their purpose in serving. Large scale events like the Open Houses, the Republic of Singapore Air Force's (RSAF) participation in the Singapore Airshow, and exhibitions in the heartlands also bring up the public standing of the Singapore military, fueling the intangible rewards for the soldiers.

With each element of the POWERS framework defined, we see the importance and relevance of drawing reference from civilian employee retention models and adding context based on the military setting and demographics of the target audience. The next step is to apply the framework to practice. The SM is one of the most powerful tools in communication, and with the more expressive and eloquent Gen Y dominating the main population within the SAF, it is useful to tap on SM to engage the military employees.[27]

The POWERS framework, in its current form, is a useful reference for military communication practitioners and commanders when designing communication messages for the military employees.

COMMUNICATING WHERE IT CLICKS – A SOCIAL MEDIA ENGAGEMENT STRATEGY

It is undeniable that Singapore has high internet penetration and SM penetration rates. According to a marketing research firm, Hashmeta's statistics, 79% of Singapore's population are internet users and the SM penetration rate is 84% – almost doubling the global average of 42%.[28] To communicate where it clicks, the SAF should continue to use Facebook (FB) as it is one of the better received SM platform in Singapore (See *Figure 3*).

Coding List for POWERS
Receptiveness to ideas, Leadership and management style, Rigid policies, Clear direction or guidance, Continuity and leadership renewal, Empathetic superiors, Perceived performance level, and Recognition. *(8 codes)*
Duty to country, Transparency of performance ranking, Career prospects, and Obligatory service. *(4 codes)*
Job satisfaction, Career progression, Work-life balance, Friendship at work, Manpower strain, and Conducive working environment. *(6 codes)*
Meaningful job, Engagement by senior management, Development opportunities, and Comprehensive system of performance measurement. *(4 codes)*
Remuneration, Mandate to command, Fulfilment of aspirations, Meeting personal expectations, Opportunities for growth, Childhood dream, and Realisation of potential. *(7 codes)*
Social responsibilities, Public impression, and Ambassador for defence. *(3 codes)*

Figure 4: The coding list for POWERS lists the keywords from a pilot study interviewing six respondents in the SAF across three services. The codes should be used to measure the strength of each communication effort (e.g. FB post), measuring in context the score across each element. For example, a post might score 75% or 0.75 when it covers 2 out of 4 codes for Organisational Commitment when it profiles a personnel who rose to rank in the career through his commitment to serve the country, highlighting the achievements.

With the platform chosen, and a framework to adopt, the approach will be a reverse-engineer of a qualitative content analysis—using key words and a coding list to categorise the standing of a communication effort using the POWERS framework. While a standardised coding can ensure uniformity in its application across the six elements of POWERS, it is inherently impossible for a single communication effort to score across all six elements uniformly. The context of each communication effort would vary, and POWERS framework has to be applied with the context in mind. It is also important for practitioners to use the guiding questions (as listed in *Figure 2*) and coding list (See *Figure 4*) to measure the strength of each element for each communication tranche, and balance the engagement as required. Real-life situations will also, inevitably, cause the levels for each element to rise and fall.

When the public standing of SAF and the commitment to defence by individuals could be affected, it is important to design communication messages to bring up the Organisational commitment and Social involvement. The means of using FB as a communication tool in 2011 might not have served its purpose better than internal communication through the commanders as the SAF's use of SM platforms like FB only took prominence after 2011. With the current followership of the MINDEF/ SAF FB pages (See *Figure 5*), FB will continue to be a platform for the SAF to engage both the internal and public audience.

RECOGNISING THE LIMITS – LIMITATIONS AND IMPLICATIONS

While SM trends might change with innovation and shifts in technology, the internal engagement framework which POWERS could offer would be more enduring if it is further developed and put through rigorous validations. Market experts have already speculated the decline of FB by 2020, hence it is important that the military continue to ride on trending platforms to reach out to its intended audience.[29]

The POWERS framework, in its current form, is a useful reference for military communication practitioners and commanders when designing communication messages for the military employees. This is especially the case when Gen Y is beginning to dominate the population in the military. With the higher thirst for information and need to express themselves, the POWERS framework becomes an emergent framework for internal engagement and employee retention. The POWERS framework's matrix and code list could be further developed to enhance its application in various contexts, and provide an easy scale for measuring the effectiveness of SM posts or communication campaigns.

MINDEF/ SAF FB Page	Followership	Managing Agency
Cyberpioneer	120,846	MINDEF Communications Organisation
The Singapore Army	140,355	Army Information Centre
Republic of Singapore Navy	143,082	Navy Information Centre
Republic of Singapore Air Force	220,343	Air Force Information Centre

Figure 5: The current followership of the four main FB pages from MINDEF/SAF.

CONCLUSION

Without effective communication, employees will be disengaged and misaligned from organisational objectives. The well-established civilian employee retention models are the closest references the military would have, and the application would have to be contextualised to the military, a non-profit organisation. Recognising the characteristics of the military employees and the opportunities and medium SM platforms offer, the POWERS framework is a distillation of key factors of employee retention in the military context from existing military and civilian employee retention models, with consideration for its application in various platforms including SM. There is room for further research and investigation to advance the POWERS framework into a prescribed framework for military communication practitioners and commanders.

ENDNOTES

1. Brainy Quote, James Humes , https://www.brainyquote.com/quotes/james_humes_154730
2. John Capon and Oleksandr S. Chernyshenko, "Applicability of civilian retention theory in the New Zealand military," New Zealand Journal of Psychology, 36 (2007): 50 – 56.
3. Cunha, Jesse M., Jeremy Arkes, Paul B. Lester, and Yu-Chu Shen. "Employee retention and psychological health: evidence from military recruits." *Applied Economics Letters* 22, no. 18 (2015): 1505-1510.

   Smith, David G., and Judith E. Rosenstein. "Gender and the Military Profession Early Career Influences, Attitudes, and Intentions." *Armed Forces & Society* (2016): 0095327X15626722.
4. Devi, V.R., "Employee Engagement is a Two-way Street," *Human Resource International Digest*, Vol 17 (2) (2009): 3-4.
5. John Capon and Oleksandr S. Chernyshenko, "Applicability of civilian retention theory in the New Zealand military," New Zealand Journal of Psychology, 36 (2007): 50 – 56.
6. Aziz, M.A. (2014). *Republic has second highest social penetration rate with 59%, more than double the global average of 26%* [Online]. Available: http://www.todayonline.com/tech/singapore-among-most-active-social-media-report [2016, Feb 5]
7. Krueger, G. P. (2001). Military psychology: United States. [Online]. Available: http://www.internationalmta.org/Documents/2004/204017P.pdf [2015, Dec 20].
8. Sucharski, I.L. and Rhoades, L., "Perceived Supervisor Support: Contributions to Perceived Organizational Support and Employee Retention," *Journal of Applied Psychology*, Vol 87 (2002): 565 – 573.
9. Paul, Pamela. "Getting inside gen Y." *American Demographics* 23, no. 9 (2001): 42-49.
10. Eisenberger, R., Stinglhamber, F. & Vandenberghe, C. "Perceived Supervisor Support: Contributions to Perceived Organizational Support and Employee Retention." *Journal of Applied Psychology*, Vol 87 (3) (2002): 565-573.
11. Ibid., 565-573.
12. Hromkovič, Juraj. "Dissemination of information in communication networks: broadcasting, gossiping, leader election, and fault-tolerance". *Springer Science & Business Media*, 2005.
13. Short, J., Williams, E., and Christie, B. "The Social Psychology of Telecommunications", *Wiley, London*, 1976.
14. Wright, D.K. & Hinson, M.D. "How new communications media are being used in public relations: A longitudinal analysis". *Public Relations Journal*, 4(3) (2010): 1-27.
15. Eisenberger, R., Stinglhamber, F. & Vandenberghe, C. "Perceived Supervisor Support: Contributions to Perceived Organizational Support and Employee Retention." *Journal of Applied Psychology*, Vol 87 (3) (2002): 565-573.
16. Steers, R.M. "Antecedents and outcomes of organizational commitment." *Administrative Science Quarterly*, 22 (1977): 46-56.
17. Allen, N.J. and Meyer, J.P. "The Measurement and Antecedents of Affective, Continuance and Normative Commitment to the Organization." *Journal of Occupational Psychology,* Vol. 63 (1990): 1-18.

18. John Capon and Oleksandr S. Chernyshenko, "Applicability of civilian retention theory in the New Zealand military," New Zealand Journal of Psychology, 36 (2007): 50 – 56.

19. Tett, R. & Meyer, J. "Job satisfaction, organizational commitment, turnover intention and turnover: Path analyses based on meta-analytical findings." *Personnel Psychology*, 46 (1993): 359-393.

20. Ibid., 359-393.

21. Griffeth, R.W., Hom, P.W. & Gaertner, S. "A meta-analysis of antecedents and correlates of employee turnover." *Journal of Management*, 26 (2000): 463-488.

22. Sunil, R. "A Review of Employee Motivation Theories and their Implications for Employee Retention within Organizations." *The Journal of American Academy of Business, Cambridge*, 5 (2004): 52-63.

23. Heneman, Herbert G., and Donald P. Schwab. "Evaluation of research on expectancy theory predictions of employee performance." *Psychological Bulletin* 78, no. 1 (1972): 1.

Lindner, James R. "Understanding employee motivation." *Journal of extension*36, no. 3 (1998): 1-8.

O'Connor, Edward J., Lawrence H. Peters, Abdullah Pooyan, Jeff Weekley, Blake Frank, and Bruce Erenkrantz. "Situational constraint effects on performance, affective reactions, and turnover: A field replication and extension." *Journal of Applied Psychology* 69, no. 4 (1984): 663.

Sunil, R. "A Review of Employee Motivation Theories and their Implications for Employee Retention within Organizations." *The Journal of American Academy of Business, Cambridge*, 5 (2004): 52-63.

24. Heneman, Herbert G., and Donald P. Schwab. "Evaluation of research on expectancy theory predictions of employee performance." *Psychological Bulletin* 78, no. 1 (1972): 1.

25. Lawler, Edward E., Lyman W. Porter, and Allen Tennenbaum. "Managers' attitudes toward interaction episodes." *Journal of Applied Psychology* 52, no. 6p1 (1968): 432.

26. Terence Ngu, Social Media Landscape in Singapore 2018, 8 August 2018, https://hashmeta.com/blog/social-media-landscape-in-singapore-2018/

27. Kietzmann, Jan H., Kristopher Hermkens, Ian P. McCarthy, and Bruno S. Silvestre. "Social media? Get serious! Understanding the functional building blocks of social media." *Business horizons* 54, no. 3 (2011): 241-251.

28. Terence Ngu, Social Media Landscape in Singapore 2018, 8 August 2018, https://hashmeta.com/blog/social-media-landscape-in-singapore-2018/

29. "Why Facebook is in Decline." Michael Spencer. 30 Sep 2015. Accessed February 22, 2016. https://www.linkedin.com/pulse/facebook-dying-michael-spencer

MAJ(NS) Tan Kok Yew is the Assistant Director (Operations and Communications) for a Small and Medium sized Enterprise, and Senior Researcher for Black Dot Research Pte Ltd. He was awarded the SAF Academic Training Award for his Bachelor of Business (Information Technology) and subsequently graduated from NTU with a Masters of Mass Communication. MAJ(NS) Tan will commence his PhD studies in Monash University, Melbourne in 2019. An Air Warfare Officer (C3) by vocation, MAJ(NS) Tan last held the appointment of Officer Commanding in 203 SQN, Air Surveillance and Control Group.

BEYOND SAF50: MAINTAINING THE SAF'S EDGE AMIDST GLOBAL, REGIONAL AND DOMESTIC CHALLENGES

by **MAJ James Yong Dun Jie**

Abstract:

The SAF has undoubtedly served its purpose in deterring potential adversaries for the past five decades. This has also allowed Singapore to gain the confidence of foreign nations, resulting in continued economic growth. The participation of the SAF in multinational operations has also forged partnerships with countries, which promoted the growth of defence diplomacy. All this were attributed to Singapore's ability to react to the ever-changing strategic landscape thus far. This essay analyses the emerging trends from the three domains—global, regional and domestic—and the potential challenges that may dull the SAF's edge. With the rise of hybrid warfare, geopolitical tensions, alongside a shrinking population, the author discusses how the aforementioned factors could impact Singapore, and offer recommendations on how the SAF can remain relevant to national defence as well as to act as a stabilising anchor for Singapore.

Keywords: Hybrid Warfare; Cyber Security; Territorial Dispute; Defence Relations; Shrinking Manpower

INTRODUCTION

Maintaining a strong defence force has been crucial in ensuring Singapore's survival and the protection of her core interests for the past 50 years. First, since independence, a capable and ready SAF has served to deter potential adversaries from exercising any ill intentions on Singapore as a sovereign and independent state. Second, it has also provided a bedrock of stability and confidence for continued foreign investments and economic growth in Singapore. Third, in contributing as a useful partner in many multinational operations, the SAF has enabled Singapore to punch above its weight internationally and lend weight to Singapore's voice in the international arena. In the words of founding Prime Minister Lee Kuan Yew in 2012: "From the day we started, I knew that we needed a strong SAF and I believe that still remains today. Without a strong SAF, there is no economic future, there is no security."[1]

Today, the SAF prides itself on being the most technologically advanced military in Southeast Asia, and on having troops with high levels of readiness and commitment to the SAF's missions. These qualities, which provide the SAF with an exceptional edge, will continue to be essential for Singapore's defence, continued economic growth, and international success. After the recent commemoration of SAF50, and as Singapore embarks on the SGfuture series of discussions, it is also timely for the SAF to think about its future beyond SAF50, so as to stay relevant amidst a transforming strategic landscape. This essay examines emerging trends from three domains—Global, Regional, and Domestic—that pose

challenges to maintaining the SAF's edge, and offers some recommendations on the way forward.

The tactics of irregular warfare can include cyber warfare, terrorism, disinformation, and other non-military means which target civilian population and infrastructure directly.

THE RISE OF HYBRID WARFARE – A GLOBAL CHALLENGE

Events such as Russia's annexation of Crimea and the emergence of the Islamic State in Iraq and Syria (ISIS) terrorist group have sparked international security concerns and implied that future conflicts against states would most likely come in the form of 'Hybrid Warfare'. Academic Frank Hoffman defined Hybrid Warfare as warfare that blends 'the lethality of state conflict with the fanatical and protracted fervour of irregular warfare.'[2] The tactics of irregular warfare can include cyber warfare, terrorism, disinformation, and other non-military means which target civilian population and infrastructure directly. Take Russia's annexation of Crimea for example. Prior to the annexation, while there were over 80,000 Russian troops and hundreds of tanks amassed at Ukraine's border, the main combatants were actually masked, unidentified rebels within Ukraine, allegedly armed with Russian military equipment, attacking key buildings and military facilities. On the cyber front, there was an active information campaign on social media which spread disinformation and caused disunity among the population. A cyber crime gang was also uncovered distributing targeted malware to Ukrainian governmental organisations in September 2014. However, it was convenient for Moscow to

A building in Marawi is set ablaze by airstrikes carried out by the Philippine Air Force during the Battle of Marawi.

dismiss the perpetrators as self-acting 'patriotic hackers' and maintain deniability.[3] The example of Ukraine reveals the following observations: Hybrid Warfare poses threats from multiple fronts, blurs the distinction between peace and war, and it can be difficult to identify a clear enemy at times.

ISIS as a Long-Term Security Threat

Besides the potential for states to wage Hybrid Warfare, Hybrid Warfare can also be waged by non-state actors. ISIS has recently been identified as a long-term security threat that may take many decades to combat.[4] Not only has the group seized large swathes of territory in Iraq and Syria as part of ISIS's vision to establish an Islamic Caliphate, it has also declared external provinces in countries such as Egypt, Libya, Algeria, Yemen and Nigeria.[5] Closer to Singapore, ISIS has ambitions to declare satellite states of its envisioned caliphate in eastern Indonesia and the Sulu archipelago of the Philippines, from which it intends to mount operations that mirror those of the ISIS core in Syria and Iraq into the Philippines and Malaysia.[6]

Perhaps a bigger threat from ISIS stems from its ability to export its ideology and violence worldwide through an information campaign marked by an adept use of social media. This has caused a rise in the numbers of self-radicalised individuals, inspired terrorist attacks on Western societies and seemingly revived Jihadist Terrorism. Recent examples included the co-ordinated attacks across Paris in November 2015, shootings in San Bernardino in December 2015, and bombings and gunfights in Jakarta in January 2016. The recent arrest of 27 radicalised Bangladeshi workers in Singapore under the Internal Security Act (ISA) serves as a reminder that the threat of self-radicalisation is real and near. While the workers had initially planned attacks targeting Bangladesh and other countries, they could have easily changed their minds and attacked Singapore instead.[7]

Impact on the SAF

Today, the SAF enjoys a strong reputation of being proficient in conventional warfare. It prides itself on being the most technologically advanced military in Southeast Asia, and on having troops with high readiness and commitment to the SAF's missions, augmented with the support of National Servicemen (NSmen). However, with the advent of Hybrid Warfare, the SAF's military edge may be eroded as adversaries apply irregular tactics to attack the SAF's perceived weaker areas to overcome our traditional strengths. Learning from precedent overseas, adversaries may employ proven methods of Hybrid Warfare such as (1) disrupting the networks the SAF depends on for operations; (2) utilising cyber warfare to steal vital military secrets and insert malware or viruses to cripple our systems; and (3) engaging in information campaigns to discredit the SAF and promulgate undesired narratives, so as to erode the public's confidence and trust in the SAF. Moreover, such perpetrators of Hybrid Warfare are likely to hide behind a veil of anonymity, not openly declaring war, and targeting non-military aspects of societies as well, including harming the civilian population directly. As such, any effective strategy against Hybrid Warfare would require the SAF to be prepared militarily, and simultaneously augment the national Whole-of-Government (WoG) efforts to strengthen all aspects of society.

GEARING UP AGAINST HYBRID WARFARE

Build Up Cyber Defence Capabilities

For the SAF to be prepared militarily, it is essential to build up sufficient cyber defence capabilities to guard against the irregular tactics likely to be employed by the perpetrators of Hybrid Warfare. The advent of network-centric warfare and military

Assets from the Republic of Singapore Navy, Police Coast Guard, Singapore Civil Defence Force, and Maritime and Port Authority of Singapore working together to deal with a hijacked merchant vessel at the sea deployment exercise.

technology means that multiple warfighting platforms will become increasingly interconnected. The tactical networks which link sensors with shooters, air-men with army troops, and Command Post situation picture with executive units, will require more protection than ever before so as to ensure SAF's mission success. The set-up of the Cyber Defence Operations Hub (CDOH) in the SAF to defend Ministry of Defence (MINDEF)/SAF networks against Cyber threats was a step in the right direction.[8] Moving forward, the SAF should deepen its cyber defence capabilities to provide comprehensive cyber protection covering all tactical-level networks and equip every serviceman with high levels of cyber security awareness and education.

Maintain Strong Conventional Forces

Even as the SAF increases its emphasis to grow nascent areas, it is important to remember the SAF's core function as a deterrent force and maintain strong conventional war capabilities. It is also noteworthy that the fight against ISIS in the Middle East by the United States-led (US) global coalition had required conventional military assets such as fighter aircraft, reconnaissance platforms and ground troops. The global ambitions of ISIS and potential formation of satellite states or military strongholds in Southeast Asia may also require regional countries to contribute military assets to defeat ISIS militarily in the future.

Contribute to Whole-Of-Government Approach

To address the threat of Hybrid Warfare targeting the entire nation, Singapore had started out on the right footing since 1984, when it adopted the Total Defence framework as its comprehensive defence strategy. Such a strategy, when implemented in its full measure, would be effective against Hybrid Warfare, which has been described as the 'exact antagonist of Total Defence.'[9] According to Defence Minister, Dr Ng Eng Hen, Hybrid Warfare seeks to "fracture the solidarity of the target nation through undermining its defences in civil, economic, social, psychological and military spheres."[10] Singapore's way forward is thus a WoG approach to build resilience in all sectors of society. Looking ahead, the SAF should look to increase its co-operation with Home Team agencies in dealing with national security threats. The series of exercises such as Exercise Northstar and Exercise

Highcrest that the SAF conducts regularly with multiple civil agencies to hone the nation's ability to deal with terrorism are a good way forward.[11]

Through building strong bilateral relationships and having regular interactions with other militaries, Singapore has been able to shape a stable and peaceful regional security architecture 'by fostering understanding, building confidence, and facilitating practical co-operation between militaries to tackle common security challenges.'

Make Full Use of National Service

As countering Hybrid Warfare would require the involvement of the entire population, National Service (NS) serves as a good opportunity to equip every Singaporean male with the relevant skills and right psychology. Beneficial knowledge and skills to impart to every serviceman can include: performing Cardio-Pulmonary Resuscitation (CPR); knowing how to respond in a terrorist attack; developing good habits to safeguard cyber security; and understanding the purpose and importance of a strong SAF so that every serviceman help defend against hostile information campaigns.

BIG POWER RIVALRY AND GEOPOLITICAL TENSIONS – REGIONAL CHALLENGES

Regionally, Southeast Asia has seen simmering tensions over the last few years, marked by territorial disputes in the South China Sea, rising military expenditures, and big powers jostling for influence and support from the different countries in the region. Within the Association of Southeast Asian Nations (ASEAN), China has disputes with the Philippines, Vietnam, Malaysia and Brunei over the ownership of several islands in the South China Sea. While each claimant nation has its own reasons to justify sovereignty over the contested territories, it is predominantly the rhetoric and actions of the two big world powers—the US and China—that affect the region and require delicate political manoeuvring from non-claimant countries. China primarily claims sovereignty over the seas and islands in a large part of the South China Sea within a 'nine-dash line' defined by a historical map released in 1947.[12] As part of asserting control, China has been conducting naval patrols and building infrastructure around these contested territories. The US, on the other hand, resolutely opposes any unlawful sovereignty claims, and advocates the freedom of navigation in international waters. In order to maintain influence and safeguard core interests in the region, each big power engages different countries in the region in its own ways, both militarily and economically.

Singapore's foreign policy with the US and China has been one of pragmatic hedging between the two powers to retain maximum flexibility.[13] Relations with China is driven primarily by economic reasons, since China is Singapore's largest trading partner and the rise of China as an economic superpower presents great potential as an export and investment destination. With the US, however, security reasons prevail. Singapore views the US presence in the region as a stabilising anchor that makes the region conducive for trade and economic growth. Potential big power rivalry may exert undesirable pressure on Singapore to abandon its neutral stand and take sides in certain sensitive issues. These pressures, if not skilfully managed, may cause defence relations with one or more countries to sour.

Republic of Singapore Air Force (RSAF) personnel unloading the humanitarian supplies in Vientiane, Laos.

Impact on the SAF

More specifically, for the SAF, good US-Singapore relations have enabled the SAF to acquire leading edge military technology and helped sustain the SAF's technological edge in the region. The US also provides the SAF with numerous overseas training locations, and invaluable knowledge transfer in the areas of technical expertise and military organisation. In recent years, however, the US, keen to deepen its security engagement in the region to balance against the rise of Chinese military assertiveness, has sought to improve defence ties with some Southeast Asian countries by offering the sales of advanced arms. Some examples included (1) the sales of the AH-64 Apache, the most advanced multi-role combat helicopter for the US Army, to Indonesia in 2013; and (2) the sales of AIM-120C7 Advanced Medium-Range Air-to-Air Missile (AMRAAM), the US's most advanced Beyond Visual Range (BVR) fighter aircraft missiles available for export, to Malaysia in 2015.[14] Such arms sales may erode the SAF's traditional technological edge in the region, and raise concerns about the effectiveness of Singapore's deterrence in the near future.

KEEPING THE SAF RELEVANT AND USEFUL

Amidst all the regional developments, the need for Singapore to maintain good defence relations with her valued partners will always remain and is even more important in current times. Conducting good defence diplomacy has always been one of Singapore's traditional strengths. Through building strong bilateral relationships and having regular interactions with other militaries, Singapore has been able to shape a stable and peaceful regional security architecture 'by fostering understanding, building confidence, and facilitating practical co-operation between militaries to tackle common security challenges.'[15] Moving forward, Singapore and the SAF can deepen our participation in international co-operative security efforts, and also grow our local defence industry to top-notch levels to maintain Singapore's status as a relevant and useful defence partner.

Contribute To Co-operative Security Efforts

First, Singapore can build closer defence relations with other countries and enhance her international standing when the SAF contributes meaningfully to international security, especially in the areas of Peace Support Operations (PSO) and Humanitarian Assistance Disaster Relief (HADR). Notable examples of PSO included joining (and sometimes helming) the international Combined Task Force 151 (CTF-151) in counter-piracy efforts in the Gulf of Aden since 2009, and contributing to reconstruction efforts in Afghanistan in 2007, and in Iraq during 2003 to 2006.[16] In terms of HADR, the SAF's deployments included contributing to firefighting operations in the forests of Sumatra and Chiang Mai in 2015, delivering relief aid to earthquake-hit Nepal in April 2015, and deploying naval and air assets to assist in the search for missing flights QZ8501 and MH370 in 2014.[17] More recently, in the global counter-terrorism combat against ISIS, Singapore has also deployed highly useful capabilities such as the Air-to-Air Refuelling KC-135R platform, and an Imagery Analysis Team to the global coalition against ISIS.[18]

Going forward, the SAF should maintain its strong competencies in Operations other than War (OOTW) and other niche areas which are useful for international deployments, and step forward readily to offer assistance whenever an opportunity presents itself. This would ideally place us high on the international arena as a preferred defence partner and give us the opportunities to have continued access to the high-end technology of leading militaries.

The recent arrest of 27 radicalised Bangladeshi workers in Singapore under the ISA serves as a reminder that the threat of self-radicalisation is real and near.

Lead Development of Future Secret-Edge Technology

Second, there is strong potential for the local defence industry to attain top-notch status in the world military technology community if it keeps up its stellar record of past successes. According to former Chief Defence Scientist (CDS) Quek Tong Boon, the SAF's real edge comes from "our ability to adapt, modify or upgrade what we can buy to better suit our requirements and environment, and, when necessary, to build what we cannot buy."[19] Beyond upgrading existing platforms such as fighter aircraft and ships, the local defence industry has also developed world-class weapon systems such as the Singapore Light Weight Howitzer (SLWH) Pegasus, SAR21 Assault Rifle, the *Endurance* Landing Ship Tank (LST), and BIONIX Armoured Vehicle Launched Bridge (AVLB), among many others.[20] Looking ahead, if Singapore is unable to secure leading-edge technology from top militaries due to regional geopolitical developments, the local defence industry would have to step up to provide the leading-edge technology the SAF needs, akin to what the defence industries in major superpowers like the US and Israel are doing. The strong potential of the local defence science community to achieve this vision was firmly acknowledged when Dr Ng Eng Hen referred to this community as the SAF's 'secret edge weapon.'[21]

Having a top-notch local defence industry will also elevate Singapore's status as a desirable partner which is able to collaborate with the world's most advanced militaries on the joint development of future secret-edge technology as well. This would forge strong defence relations with major militaries and also grant the SAF access to the new technology after it is developed.

UNFAVOURABLE DEMOGRAPHICS – A DOMESTIC CHALLENGE

Locally, Singapore's demography has often been proclaimed as the biggest challenge facing the SAF. According to Defence Minister, Dr Ng Eng Hen, the number of full-time NSmen will fall by around 30 percent from 2015 to 2030, in line with the falling number of resident live-births from 49,787 in 1990 to 35,129 in 2010.[22] This reduction in live-births which contributes to the manpower pool from which the SAF derives its regular force and NSmen reserves, would significantly affect the SAF's future force structure. If the amount of work to be done remains the same, the 30 percent reduction in future manpower would mean that each soldier in 2030 would have to do roughly the same amount of work as what 1.5 soldiers can do today.

A second demographic trend to note is the steady rise in the life expectancy of a Singapore resident, from 75.3 for a person born in 1990, to 81.7 for one born in 2010 (and this is still increasing for those born later).[23] An increase in the number of workable years is likely to result from the increase in life expectancy. While this may help to augment the shrinking manpower pool in the future, there is also a challenge of changing career aspirations brought about by this trend. This is due to the relatively young retirement age in the SAF career vis-à-vis the projected increase in 'workable years.' As people expect to live longer, and hence want to work longer to build up sufficient retirement savings, they may shun away from a SAF career so that they can pursue another career with a later retirement age.

A third demographic trend of significance is the change in the social construct of the population, as the government seeks to grant citizenship to between 15,000 and 25,000 foreigners each year and give permanent resident (PR) status to 30,000 foreigners yearly to supplement the size of the population.[24] This is done in order to ensure a strong and sustainable Singaporean core for the longer-term future. This trend poses considerable qualitative impact on National Service (NS) and the SAF's future manpower construct. Children of new citizens and PRs may not be as committed and attached to the country as children brought up by families which have lived in Singapore for several decades. This may result in a diluted commitment to defence in the future, and reduce the effectiveness of the defence force.

INNOVATING FOR FUTURE EFFECTIVENESS

To address the challenges brought about by the inevitable demographic trends, the SAF needs to continue its keen spirit of innovation, beyond improving daily operations, to focus more on: (1) infusing ground-breaking technology; and (2) reshaping manpower policies.

Operate with Robotic Technology

The first demographic trend of falling resident live births presents a quantitative challenge to the SAF in meeting the numbers required for future operations, and the way forward would be to utilise technology. This would enable each soldier to do much more than what he or she is capable of now. Beyond adopting newer platforms which require lesser manpower to operate, the SAF is also looking at combining manned platforms with more unmanned systems so as to optimise the efforts of a leaner future force.[25] Some examples can be seen in the 'The Future of Us' exhibition, which touted possibilities of unmanned vessels taking over all area surveying functions, and smart, robotics technologies that are capable of autonomous operations.[26] Working with unmanned systems presents new operating paradigms to the SAF, and it is important to prepare soldiers well over the next few years to embrace this innovative change.

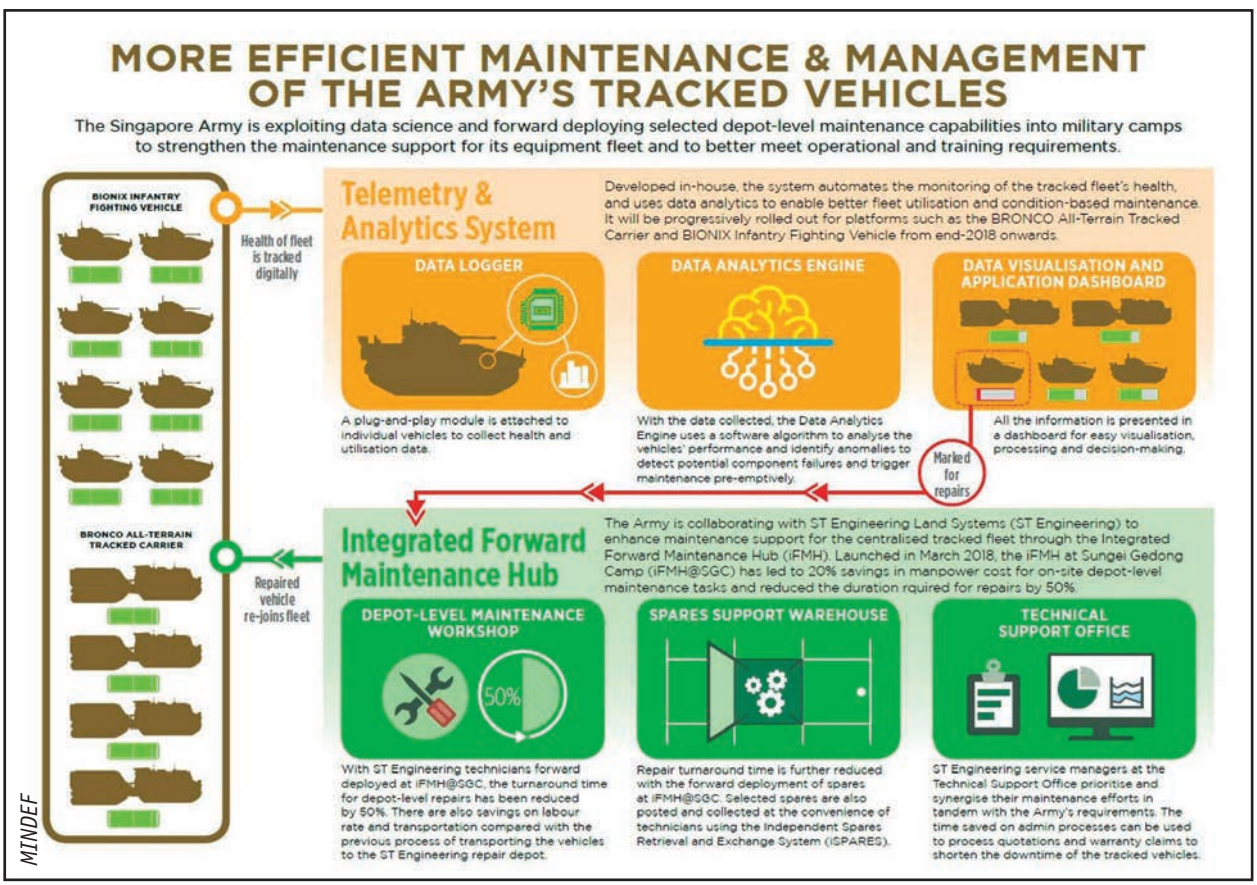
SHAPE MANPOWER POLICIES THAT EMBRACE DEMOGRAPHIC TRENDS

The second and third demographic trends posed qualitative challenges of changing career aspirations and a diluting commitment to defence respectively. It would require a re-branding of the SAF career to bring about a mindset change. Such a re-branding may need to incorporate people's preference for longer career lifespans across all career schemes, or open up more opportunities for non-traditional recruitment pools such as women and mid-careerists. To address the changing social construct of the future manpower pool, PRs and new citizens would have to be better integrated into the NS system. Recruitment policies may also have to be altered to allow this group of people to participate beyond the SAF Volunteer Corps (SAFVC), and join the SAF as regulars, so as to meet the numbers required for the future force.

Having presented these recommendations, the essay also acknowledged that these emerging demographic trends are not that straightforward to address, and the SAF may require more thinking and information-gathering before manpower policies can be shaped appropriately to resolve these challenges.

CONCLUSION

To conclude, for the past 50 years, the SAF had performed exceptionally well as a deterrent force, as a stabilising anchor for Singapore's economy, and as a reliable partner in international deployments. This has given strength to the nation and enhanced Singapore's standing internationally. Moving past SAF50, it is essential to maintain the SAF's traditional strong



An infographic depicting the Smart Army Camp of the Future.

edge in the region to continually protect Singapore's independence and interests as a small island-state. This essay has examined some emerging trends of concern that posed challenges to maintaining the SAF's edge: the global rise of Hybrid Warfare which has radically changed the nature of modern warfare; regional geopolitical tensions and big-power rivalry which has posed diplomatic challenges and threatened to erode the SAF's technological edge over time; and domestic demographic trends which would influence the use of technology and manpower construct of the future SAF.

Whether the SAF can continue to sustain its edge in the region will depend on how well it addresses these challenges. Moving forward, it is important for the SAF to gear up against Hybrid Warfare by building up cyber defence capabilities, maintaining strong conventional forces, making full use of NS, and contributing to the national WoG approach. To sustain good defence relations and maintain its technological edge, the SAF can keep itself relevant and useful to its valued partners by continuing its deliberate and meaningful contributions to co-operative security efforts, and taking a lead in the development of future secret-edge technology with the local defence industry. Lastly, to address the inevitable demographic challenges, innovating for future effectiveness will be of strong interest to the SAF as it looks towards operating with robotic technologies, and shaping manpower policies that embrace the demographic trends.

ENDNOTES

1. Koh Eng Beng, "In remembrance: Lee Kuan Yew", *Cyber Pioneer*, last modified 23 Apr 2015, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2015/may15_fs1.html#.VrbVEvl97IV
2. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: *Potomac Institute for Policy Studies*, pg 58. Accessed 12 February 2016. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
3. Eve Hunter and Piret Pernik, "The Challenges of Hybrid Warfare" *International Centre for Defence and Security*, April 2015, accessed 12 February 2016, http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf
4. Jermyn Chow, "Jakarta 'on right track' in fight against terror", *The Straits Times*, last modified 26 January 2016, http://www.straitstimes.com/asia/se-asia/jakarta-on-right-track-in-fight-against-terror
5. Karen Yourish, Derek Watkins and Tom Giratikanon, "Recent Attacks Demonstrate Islamic State's Ability to Both Inspire and Coordinate Terror", *The New York Times*, 14 January 2016, http://www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html?_r=0
6. Rohan Gunaratna, "ISIS in Philippines a threat to region", *The Straits Times*, last modified 12 January 2016, http://www.straitstimes.com/opinion/isis-in-philippines-a-threat-to-region
7. Lee Min Kok, "27 radicalised Bangladeshis arrested in Singapore under Internal Security Act: MHA", *The Straits Times*, last modified 21 January 2016, http://www.straitstimes.com/singapore/courts-crime/27-radicalised-bangladeshis-arrested-in-singapore-under-internal-security-act
8. Rachael Lim, "New hub to defend against cyber threats", *Cyber Pioneer*, last modified 30 June 2013, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2013/jun/30jun13_news2updated.html#.Vr8-c_l97IU
9. "Speech by Dr Ng Eng Hen, Minister for Defence, at Committee of Supply Debate 2015", *MINDEF*, last modified 6 March 2015, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05mar15_speech.html#.Vr8unvl97IU
10. Ibid.
11. Ong Hong Tat, "SAF and key agencies test readiness in Exercise Northstar 9", *Cyber Pioneer*, last modified

9 May 2015, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2015/may/09may15_news.html#.Vr9PMvl97IU

Rachael Lim, "New hub to defend against cyber threats", *Cyber Pioneer*, last modified 30 June 2013, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2013/jun/30jun13_news2updated.html#.Vr8-c_l97IU

12. "Q&A: South China Sea dispute", *BBC News*, last modified on 27 October 2015, http://www.bbc.com/news/world-asia-pacific-13748349

13. Cai Dexian, "Hedging for Maximum Flexibility: Singapore's Pragmatic Approach to Security Relations with the US and China", Pointer Volume 39, No. 2, last modified 23 July 2013

14. Ellis Taylor, "Boeing awarded Indonesian Apache contract", *FlightGlobal*, last modified 27 January 2015, https://www.flightglobal.com/news/articles/boeing-awarded-indonesian-apache-contract-408325/

Prashanth Parameswaran, "US Approves New Missile Deals for Indonesia, Malaysia", *The Diplomat*, last modified on 7 May 2015, http://thediplomat.com/2015/05/us-approves-new-missile-deals-for-indonesia-malaysia/

15. "Defence Policy & Diplomacy", *MINDEF*, last modified on 18 October 2012, http://www.mindef.gov.sg/imindef/key_topics/defence_policy.html

16. "Peace Support Operations", *MINDEF*, last modified on 16 March 2015, http://www.mindef.gov.sg/imindef/key_topics/overseas_operations/peacesupportops/home.html

17. "HADR Deployments", *MINDEF*, last modified on 16 March 2015, http://www.mindef.gov.sg/content/imindef/key_topics/overseas_operations/hadr/home.html

18. "Reply by Minister for Defence, Dr Ng Eng Hen, to Parliamentary Question on Singapore's Deployment of Support to the Anti-ISIS Coalition", *MINDEF*, last modified on 28 January 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/ps/2016/19jan15_ps.html#.VsAbyfl97IU

19. Ong Hong Tat, "Forging a technological edge", *Cyber Pioneer*, last modified 13 August 2010, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2010/mar10_fs2.html#.VsAwffl97IV

20. "Factsheet - The Singapore Light Weight Howitzer (SLWH) Pegasus", *MINDEF*, last modified 18 April 2006, http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2005/oct/28oct05_nr/28oct05_fs.html#.VsA0APl97IV

ST Engineering, assessed on 13 February 2016, http://www.stengg.com/products-solutions/listing-by-sector

21. "Opening Address by the Minister For Defence Dr Ng Eng Hen at the Defence Technology Community Pioneers' Dinner at Island Ballroom, The Shangri-La Hotel", *MINDEF*, last modified on 22 May 2015, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/06may15_speech.html#.VsApDvl97IU

22. "Opening Address by the Minister For Defence Dr Ng Eng Hen at the Defence Technology Community Pioneers' Dinner at Island Ballroom, The Shangri-La Hotel", *MINDEF*, last modified on 22 May 2015, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/06may15_speech.html#.VryF2Pl97IU

"Population Trends 2015", *Department of Statistics Singapore*, https://www.singstat.gov.sg/docs/default-source/default-document-library/publications/publications_and_papers/population_and_population_structure/population2015.pdf

23. Ibid.

24. Goh Chin Lian, "Goal: 15,000-25,000 new citizens a year", *The Straits Times*, modified 30 January 2013, http://www.straitstimes.com/singapore/goal-15000-25000-new-citizens-a-year

25. Kelly Ng, "SAF reorganising to tackle challenge of hybrid warfare", *TODAY*, last modified on 2 July 2015,http://www.todayonline.com/singapore/spore-modernising-defence-systems-meet-future-challenges?singlepage=true

26. Teo Jing Ting, "SAF 2030 sneak peek", *Cyber Pioneer*, last modified on 1 February 2016, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2016/feb16_fs1.html#.VsBAdfl97IU

MAJ James Yong Dun Jie is an Air Warfare Officer (Air Battle Management) by vocation. He is currently an Officer Commanding in 111 SQN, Air Combat Command. Previously, he had served as Planning Officer (Air), Joint Operations Planning Branch, in Joint Operations Department. MAJ Yong holds a Bachelors of Science (Honours) in Statistics, Economics and Finance from UCL and a Masters of Science in Operations Research from Columbia University.

UNMANNED AERIAL VEHICLES - A CLEAR AND PRESENT DANGER, AND WHAT WE CAN DO ABOUT THEM

by **MAJ Jerry Chua**

Abstract:

In this essay, the author explores how Unmanned Aerial Vehicles (UAV) have been transformed from a simple daily equipment that everyone uses, to a deadly weapon that is utilised by both military and terrorists. According to the author, there is no single solution to deal with the threat of UAVs. Possible defence concepts such as geo-fencing, high energy lasers and jamming may still not succeed. These are single solutions where a full breach would occur once that one layer was broken. The author then proposes a multi-layered approach in dealing with UAVs to provide for contingencies in the event that one layer fails. This five layer defence model comprise the concepts of Prevention, Deterrence, Denial, Detection and destruction/Interruption. With this model, the author discusses how Singapore can prevent attacks from UAVs and plan a counterattack against the aggressor.

Keywords: Multi-Layered Approach; Resilience; Conventional Barricades; Continual Vigilance; Crisis Management

INTRODUCTION

You can hear them buzzing around in the parks. You can see them being used for unique vantage points in wedding videos. You can see them displayed in all shapes and sizes in your neighbour toy shops.

With improvements in technology leading to the widespread commercialisation and tumbling prices of UAVs, quad-copters and recreational drones are now a common sight. Corporations are also swiftly catching onto the potential avenue to reduce their overheads, with Amazon announcing the 'Amazon Prime Air', a home delivery service using UAVs.

However, increased usage of UAVs is not without its downside. With their agility, small size, and ability to circumvent traditional barricades, UAVs make for a good delivery platform for more malicious packages by terrorist groups and self-radicalised individuals. Recognising the danger posed by such groups, law enforcement and national defence agencies are scrambling for possible solutions. These have ranged from high tech jammers, space age Lasers and even the unconventional employment of trained bald eagles.[1] However, effectively dealing with such threats requires more than just new weaponry, but a more comprehensive, multi-layered approach.

A ROSE BY ANY OTHER NAME

Searching for the definition of Unmanned Aerial Vehicles yields a dazzling array of results, with some even including Cruise Missiles.[2] A cursory search of the articles on UAV threats throws out several nomenclatures such as Unmanned Aerial System

(UAS), drones, Remote Controlled Aircraft (RCA) and Remotely Piloted Vehicle (RPV) that are seemingly used interchangeably.

While the terms used differ, their meanings are fairly aligned, with the Merriam-Webster dictionary defining drones as 'an unmanned aircraft or ship guided by remote control or on board computers' and UAV as a RPV.[3] The Federal Aviation Administration defines a UAS as 'the unmanned aircraft and all of the associated support equipment, control station, data links, telemetry, communication and navigation equipment, etc., necessary to operate the unmanned aircraft' and includes hobby aircraft as part of the definition. [4]

Along with the non-standard nomenclature, there are also no industry standard classifications for UAVs. However, classes such as micro- and mini- are widely used. An example of the some of the classifications can be seen below in *Table 1*:

For the purposes of this essay, the nomenclature UAV will be used, as the focus is on the platform, rather than the supporting equipment. The UAVs described in the essay are assumed to be consumer grade and widely available, belonging to the micro- and mini- classifications.

With the increased awareness of UAV threats, several sensor platforms have been designed around the detection of UAV targets.

ATTACK OF THE 'DRONES'

Law enforcement agencies including the United States (US) Department of Homeland Security (DHS) and New York Police Department (NYPD) have issued assessments and warnings that micro- and mini-UAVs could be used as tools to mount terror attacks.[5] Despite their small size and limited endurance, these UAVs' small Radar Cross Section (RCS), agility and ability to circumvent the conventional barricades make them a deadly addition to the potential terrorist's arsenal. There are three potential scenarios that a UAV attack could pan out.

Scenario 1: Individual or terrorist group flies UAVs loaded with explosives with the objective of attacking a Key Installation (KINs) or Very Very Important Person (VVIP).

Though the weight that the UAV can carry is limited, it is able to carry the explosives closer to the target area, flying over the fences and walls. This allows it to cause more damage, potentially

Category	Weight (kg)	Altitude (ft)	Endurance (hr)	Range (km)
Micro	<1	300	1	<5
Mini	<25	<10,000	1-6	<25
Close Range	<200	<15,000	4-8	<75
Small Range	<750	<25,000	8-24	<200
MALE	>1,000	<30,000	>24	>1,000
MALE +	>3,000	>30,000	>24	>1,000
HALE	>3,000	>45,000	>24	>1,000

Table 1: Classification of UAVs by Range and Endurance.[6]

triggering off secondary explosions if the target was a petroleum-chemical or nuclear power plant. In the case of the VVIP, the UAV is able to fly over the protective bulletproof glass before detonating, causing serious injury or even death.

KINs such as the White House and French nuclear power plants have been overflown UAVs before, with the latter being overflown on no less than 13 occasions.[7] The latter scenario of an attack on a VVIP could have also played out during the party campaign event when a Parrot AR.Drone flew and crashed, metres from German Chancellor Angela Merkel.[8] While these cases mentioned were resolved peacefully, such gaps in security could have been exploited by individuals with sinister intents.

Figure 1: A Parrot AR.Drone, similar to the one that flew and crashed within metres of Germany Chancellor Angela Merkel during a Democratic Party campaign event.

Scenario 2: Individual or terrorist group flies UAV loaded with Chemical, Biological, Radiological or Explosive (CBRE) agents and releases/triggers it during a crowded event.

The direct causalities are few, but the resulting panic triggers a human stampede, causing mass causalities as people rush towards the exits. While there have been no documented cases of UAV attacks triggering human stampedes, there have been several occurrences of such tragedies triggered by other reasons, notably during the Hajj in Mecca, Saudi Arabia.[9] With similar conditions of high crowd density and limited exit points, it will not be hard to imagine mass panic sweeping over the crowd following an explosion.

Scenario 3: Individual flies the UAV into the flight path of a commercial or military aircraft that is taking off or landing. The aircraft smashes into the UAV, causing injury to the pilot and damaging the aircraft, potentially causing the aircraft to crash.

As with scenario 2, there have been no documented cases of UAV strikes causing damage to an airborne aircraft. However, it was reported in the US Airspace alone, there were more than 300 cases of close proximity flights between a manned aircraft and UAV (classified as 'close encounters') between 13th December and 15th September.[10] Even without malicious intentions, the high occurrence rate of such potentially catastrophic incidents is a cause for concern.

With their agility, small size, and ability to circumvent traditional barricades, UAVs make for a good delivery platform for more malicious packages by terrorist groups and self-radicalised individuals.

CHALLENGES OF COUNTERING UAVS

Though it is generally acknowledged that UAVs pose a potential threat to security, dealing with them is not as intuitive. Due to their small RCS, low speed and flying altitude, UAVs are inherently difficult to detect and classify using conventional radar systems, as these radars were designed to filter out such plots as noise to avoid picking up birds and buildings by mistake.

Electro-Optical/Infrared (EO/IR) sensors will similarly experience problems with the picking up and tracking of such targets due to their small physical size. Additionally, the UAV's low altitude could cause its image to be blurred by the heat radiating off the top of buildings.

Even if the detection hurdle was crossed, most air defence systems, being designed for engaging conventional air threats such as combat aircraft, precision guided munitions and bombs on a large scale, are ill equipped to handle UAVs.[11] The resulting collateral damage caused by the firing of such weapons in fact, can be more than the UAV and the resulting panic can trigger off a human stampede or crush, indirectly accomplishing the intent of the attack.[12]

UAVs are also able to circumvent or fly over the most commonly used barriers such as fences, concertina wires and walls, making their point of entry unpredictable. This, coupled with their agility, means that UAVs will likely be the pop-up targets, reducing the reaction time for the authorities.

SINGAPORE IN CONTEXT

Singapore is not new to the threat of terrorism, with the terrorist group Jemaah Islamiyah (JI) revealed to have planned to attack foreign and local targets in Singapore as early as 1997.[13]

Singapore is a known target for ISIS and its supporters. In 2015, two Singaporeans were also detained under the ISA with the intention to join ISIS.[14] Singapore also resides in a volatile region, with suspected ISIS militants and supporters found in both Malaysia and Indonesia.

However, Singapore presents several other unique characteristics that makes her particularly susceptible to a UAV attack.

Firstly, with a population density of 7,736 per square kilometre, Singapore is one of the most densely populated countries in the world.[15] With our relatively small land area, our critical infrastructure and airfields are also closely located with the general populace. In particular, the flight paths of most our civilian and military aircraft either take them above populated areas, or are clearly visible to the public eye. The island is also completely urbanised, with most parts covered with high-rise buildings and estates.

With few regulations governing the sales of UAVs, these are widely available in all the toy and hobby stores in Singapore.

Putting these factors together, Singapore is a highly attractive target for UAV attacks, with a high payoff arising from the dense population and her status as one of the most secured and prosperous countries in the region. Additionally, there are readily available sources of acquiring and training on UAVs, and any planned attack will be hard to detect until the very last minute.

SINGAPORE'S MODEL FOR DEFENCE

Effectively dealing with the UAV threat requires a whole-of-government approach. In the qualitative study *'Examining Unmanned Aerial System Threats and Defences: A Conceptual Analysis'* conducted by Ryan J. Wallace and Jon M. Loffi, it was highlighted that none of the defence concepts proposed thus far were complete models. Instead, they were merely focused on single solutions where would cause a full breach in defences once that one layer was broken.[16] Consolidating and organising the various defence concepts, they developed a five layer defence in depth model (Prevention-Deterrence-Denial-Detection-Destruction/Interruption).[17] Drawing inspiration from their model, the following model for Singapore's defence against UAVs is

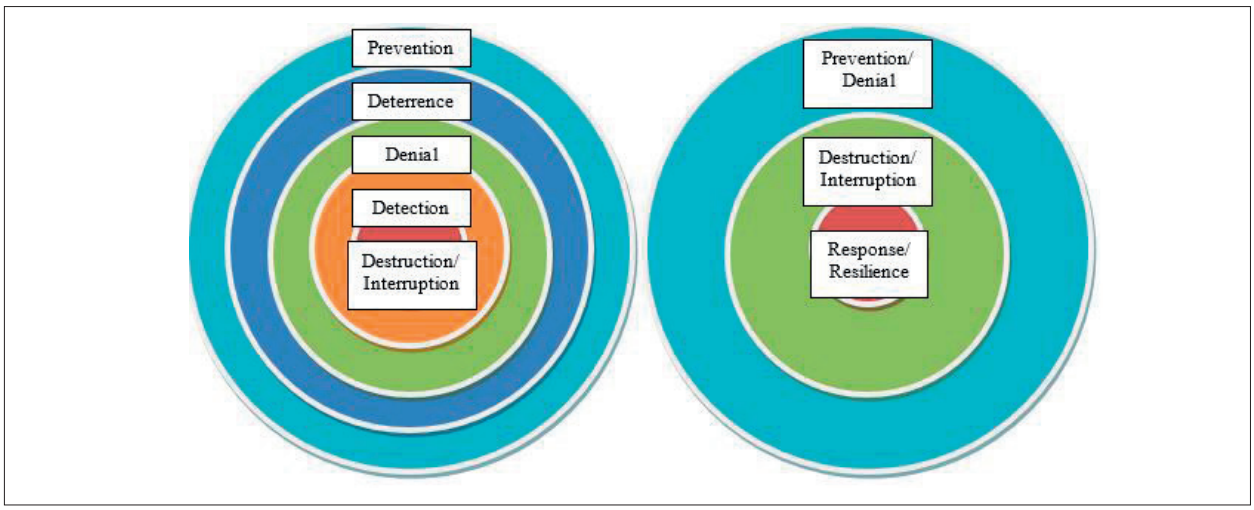


Figure 2: UAS Defence in Depth Model by Ryan Wallace, et al. (left), Proposed Model for Singapore's Defence against UAVs (right).[18]

proposed.

The outermost concentric circle of Prevention/ Denial merges encompasses all actions taken to prevent such attacks from occurring. The second circle includes all the actions to prevent such attacks from succeeding and the innermost circle describes the post-attack actions.

By putting in place and regularly practising crisis management procedures in the event of a successful terrorist attack, the various agencies will be able to respond swiftly and decisively, limiting public disruption and alarm, while bolstering confidence in the authority's ability to handle such situations.

PREVENTION/DENIAL

On the forefront of the efforts to prevent UAV attacks on Singapore soil is the continual vigilance from intelligence agencies such as the Internal Security Department (ISD), and Intelligence Departments from the Military and Police. Intelligence efforts in worldwide have been instrumental in the uncovering of plans by self-racialised individuals and terrorist groups to perform attacks using UAVs. Notable examples include (1) Rezwan Ferdaus, who plotted to carry out attacks on key US installations using remote-controlled models of the F-86 Sabre packed with explosives, (2) Al-Qaeda plot to release chemical agents in Iraq using remote-controlled helicopters, and (3) Islamic terror plot to employ UAVs (packed with explosives) as guided missiles for a planned assassination in Germany.[19]

Complementing intelligence efforts are legislative Acts that will control the flying activities of the UAVs. This includes both the enactment of the laws, and its enforcement. On the former, Singapore has taken the first step by passing the Unmanned Aircraft (Public Safety and Security) Act 2015, which amends existing Air Navigation, and Public Order Acts.[20] This act restricts the operations of UAVs in terms of UAV weight, operating height and activities, and lays down the situations where a permit must be obtained. While the Act's enactment is clearly a step in the right direction, its enforcement presents two inherent difficulties. Firstly, most mini- and micro-UAVs remain widely accessible to the public without

purchase controls. This presents opportunities for individuals to purchase and perform modifications to enhance its performance for malicious purposes. Secondly, encounters with the UAV tend to be fleeting, reducing the amount of time for authorities to detect and detain the perpetrators. Educating the public is one possible solution to mitigate the issue of enforcement. Similar to the wide-spread campaign educating the public to report suspicious bags, a campaign educating the public to report suspicious UAV flying activity could provide the authorities with 'extra pairs of eyes', and improve responsiveness.

Another potential solution is to enforce the hard-coding of navigation algorithm by the UAV manufacturers. Referred to as 'geo-fencing', this would allow the authorities to establish vital fences around the KINs, preventing the UAVs from overflying pre-set boundaries. [21]

DESTRUCTION/INTERRUPTION

Should deterrence and denial fail, and an attack is carried out, the next step is to prevent the attack from succeeding through destruction (hard kill) or interruption (soft kill).

To accomplish this, however, requires overcoming the detection hurdle. For this, the SAF could leverage on the expertise within the Air Force and Army in the sourcing and employment of sensors. With the increased awareness of UAV threats, several sensor platforms have been designed around the detection of UAV targets. One such platform is the Giraffe Agile Multi-Beam (AMB) produced by SAAB, which is allegedly able to distinguish UAVs from ground and sea clutter using its Enhanced Low, Slow and Small function.[22] While destruction could be most conveniently carried out using kinetic weapons such as firearms and Ground Based Air Defence (GBAD) assets, the resulting collateral damage and panic caused could outweigh the damage caused by the UAV itself. Additionally, due to the pop-up nature of the targets, the engagement window could be very small.

With their speed of light and projectile-less engagements, coupled with pinpoint accuracy, High Energy Lasers (HELs) could offer a potential answer. Once the subject of scepticism from US President Ronald Reagan's Strategic Defence Initiative (nicknamed 'Star Wars'), advancements in technology and defence demands have since propelled the

Figure 3: 'See Anything Suspicious' posters used by the British Transport Police to raise awareness about suspicious packages.[23]

Figure 4: LaWS is the first operationally deployed HEL weapon and is installed aboard the USS Ponce.

development of HELs, with the first operational deployment of a HEL weapon, LaWS (Laser Weapon System) on board the *USS Ponce* on 14th September.[24] The incorporation of such weapons could provide the SAF with the capability to engage and take out UAVs while minimising collateral damage.

As UAVs are controlled using radio frequencies, commonly the 2.4 GHz for the newer models and 72 MHz and for the older ones, jamming the UAV's signal could also prevent it from completing its attack.[25] Once a UAV is interrupted due to jamming, the UAV would either hover, descend to land, or return to its point of origin.[26] Battelle, a non-profit Research and Development (R&D) organisation from Ohio, has developed one such short range jammer designed against UAVs. Dubbed the *DroneDefender*, the directional jammer can allegedly jam UAV signals at up to 400 metres away and represents a potential soft kill option for law-enforcement officers guarding KINs or patrolling major events.[27]

Effectively dealing with the UAV threat requires a whole-of-government approach.

RESPONSE/RESILIENCE

While the actions pre- and during UAV attacks are critical, the post-attack actions are no less important. There may be situations where attacks have been successfully carried out and the authorities will need to take action in the aftermath to prevent future attacks from occurring. This is because terrorism's goal does not lay in the execution of the attack, but the disruption to normal life and publicity that it generates in the aftermath.[28] The key to preventing

such future attacks hence lies in the swift response of the authorities and resilience of the populace.[29]

By putting in place and regularly practising crisis management procedures in the event of a successful terrorist attack, the various agencies will be able to respond swiftly and decisively, limiting public disruption and alarm, while bolstering confidence in the authority's ability to handle such situations. In Singapore's context, Exercise Northstar serves as a good platform to practise inter-agency co-ordination and collaboration. These series of exercises have typically been modelled after successful terrorism attack and could be expanded to deal with the sightings of UAVs and human crushes.

On building resilience, the public can be educated about what they can do in the event of a terrorist attack. This allows them to play an active role rather than remain as passive observers in the aftermath. The public should also be given an accurate assessment of the possibility of a successful terrorist attack rather than fear-mongering or overly rosy messages. Over the years, Singapore has witnessed a gradual shift in the messaging from the leadership that terrorism is something that we will need to be mentally prepared for.[30]

Brian Jenkins on the RAND blog sums up the inner-most circle or Response/Resilience with, "We may have to live with terrorism, but we do not have to live in terror."[31]

CONCLUSION

When dealing with the UAV threat, there is no single 'magic bullet' or permanent solution. Geo-fencing could give way to hacking, HELs suffer from attenuation during adverse weather, jamming requires precise knowledge of the frequency band used, and building resilience takes time. Hence, it is critical for a multi-layered approach to provide for contingencies in the event that one layer fails.

One thing is clear: the proliferation of the UAVs is here to stay, and its payloads and endurance could only increase with the advancements in technology. In the fight against the malicious use of UAVs, the potential aggressors already have the tools at hand.

ENDNOTES

1. Sam Thielman. "Eagle-eyed: Dutch Police to Train Birds to Take down Unauthorised Drones." The Guardian. February 1, 2016. http://www.theguardian.com/world/2016/feb/01/dutch-netherlandspolice-birds-unauthorized-drones.
2. Dennis, Gormley. "Unmanned Air Vehicles as Terror Weapons: Real or Imagined?" Nuclear Threat Initiative (NTI). July 1, 2005. http://www.nti.org/analysis/articles/unmanned-air-vehicles-terrorweapons/.
3. "Drone." Merriam-Webster. http://www.merriam-webster.com/dictionary/drone.

   "UAV." Merriam-Webster. http://www.merriam-webster.com/dictionary/UAV.
4. "Unmanned Aircraft Systems (UAS) Frequently Asked Questions." Federal Aviation Administration. https://www.faa.gov/uas/faq/#qn1.
5. David Kravets. "Homeland Security: Hobbyist-sized Drones Are the Latest Terrorism Threats." Ars Technica. August 4, 2015. http://arstechnica.com/tech-policy/2015/08/homeland-security-hobbyistsized-drones-are-the-latest-terrorism-threats/.

   Steve Hopkins. "Drones Carrying Explosives Are the Number One Terror Threat, Say NYPD." Mail Online. October 30, 2014. http://www.dailymail.co.uk/news/article-2814363/Drones-carryingexplosives-number-one-terror-threat-say-NYPD.html.
6. "Introduction to Unmanned Aerial Vehicle (UAV)." *UAV Society* (blog). http://uavsociety.blogspot.sg/2014/06/introduction-to-unmanned-aerial-vehicle.html.

7. Schmidt, Michael S., and Michael D. Shear. "A Drone, Too Small for Radar to Detect, Rattles the White House." The New York TImes. January 26, 2015. http://www.nytimes.com/2015/01/27/us/white-house-drone.html?_r=0.

Catherine Philips, and Conor Gaffey. "Most French Nuclear Plants 'Should Be Shut Down' Over Drone Threat." Newsweek, February 24, 2015. http://europe newsweek.com/most-french-nuclear-plantsshould-be-shut-down-over-drone-threat-309019.

Ibid.

8. Sean Gallagher. "German Chancellor's Drone "attack" Shows the Threat of Weaponized UAVs." Ars Technica. September 19, 2013. http://arstechnica.com/information-technology/2013/09/germanchancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

9. Faith Karimi, and Schams Elwazer. "Stampede Kills More than 700 at Hajj Pilgrimage in Mecca." CNN. September 25, 2015. http://edition.cnn.com/2015/09/24/middleeast/stampede-hajjpilgrimage/.

10. Dan Gettinger, and Arthur Holland Michael. "Drone Sightings and Close Encounters: An Analysis." Center for the Study of the Drone. 2015. http://dronecenter.bard.edu/drone-sightings-and-closeencounters/.

11. E.C. Evans "National Air Defense: Challenges, Solution Profiles, and Technology Needs." The MITRE Corporation. October 2014. http://www.mitre.org/publications/technical-papers/nationalair-defense-challenges-solution-profiles-and-technology-needs.

12. J, Kraker K., and Wiel R. V. "Mini UAV as an Improvised Air Threat." AUVSI Unmanned Systems 2013, Washington, DC, USA, August 2013, 849-61.

13. "Operation against Jemaah Islamiyah Begins." National Library Board Singapore. http://eresources.nlb.gov.sg/history/events/90267935-71ef-4829-8faf-f6039a086cda.

14. "2 Singaporeans Detained for Planning to Join ISIS." Asia One. September 30, 2015. http://news.asiaone.com/news/singapore/2-singaporeans-detained-planning-join-isis.

15. "Population Density (people per Sq. Km of Land Area)." The World Bank.http://data.worldbank.org/indicator/EN.POP.DNST.

16. Wallace, Ryan J., and Jon M. Loffi. "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis." International Journal of Aviation, Aeronautices and Aerospace 2, no. 4 (October 1, 2015). http://commons.erau.edu/cgi/viewcontent.cgi?article=1084&context=ijaaa.

17. Ibid., 13.

18. Ibid., 13.

19. Ibid., 1.

Paul J., DR. "The Evolving Terror Threat Posed by Aerial Platforms." Mackenzie Institute. March 18, 2015. http://mackenzieinstitute.com/evolving-terror-threat-posed-aerial-platforms/.

Ibid.

20. "Unmanned Aircraft (Public Safety and Security) Act 2015." CAAS.http://www.caas.gov.sg/caasWeb2010/export/sites/caas/en/Regulations/Legislations/Unmanned_Aircraft_Public_Safety_and_Security_Act_2015.html.

21. Gareth Jennings. "DSEI 2015: Saab Demos Giraffe Radar's Counter-UAV Capabilities to UK." Janes Defence. September 16, 2015. http://www.janes.com/article/54405/dsei-2015-saab-demos-girafferadar-s-counter-uav-capabilities-to-uk.

22. Wallace, Ryan J., and Jon M. Loffi. "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis." International Journal of Aviation, Aeronautices and Aerospace 2, no. 4 (October 1, 2015). http://commons.erau.edu/cgi/viewcontent.cgi?article=1084&context=ijaaa.

23. "'See Anything Suspicious' Posters." British Transport Police. September 2011. http://www.btp.police.uk/advice_and_info/our_campaigns/see_anything_suspicious.aspx.

24. Jon Harper. "Navy Authorized to Use New Laser Weapon for Self-defense on USS Ponce." Stars and Strips. December 11, 2014. http://www.stripes.com/news/

us/navy-authorized-to-use-newlaser-weapon-for-self-defense-on-uss-ponce-1.318735.

25. "RC Frequencies at The Field." Hooked on RC Airplanes. http://www.hooked-on-rcairplanes.com/rc-frequencies.html.

26. Matt Terndrup. "Long-Distance Jammer Is Taking Down Drones." Maker Media. October 16,

2015. http://makezine.com/2015/10/16/research-company-takes-aim-uavs-portable-anti-dronerifle/.

27. Ibid.

28. Romesh Ratnesar. "As in Boston, Resilience Can Help the U.S. Defeat Terrorist Attacks." Bloomberg Business. April 18, 2013. http://www.bloomberg.com/bw/articles/2013-04-18/as-inboston- resilience-can-help-the-u-dot-s-dot-defeat-terrorist-attacks.

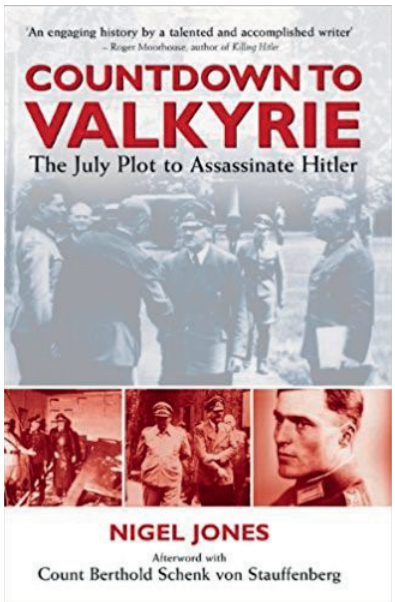
29. Jenkins, Brian Michael. "The Four Defensive Measures Against Terrorism." The RAND Blog. September 24, 2004. http://www.rand.org/blog/2004/09/the-four-defensive-measures-againstterrorism.html.

30. Walter Sim. "Be Mentally Prepared to Deal with Terror Attack If It Happens: PM Lee." The Straits Time Singapore. November 17, 2015. http://www.straitstimes.com/singapore/be-mentallyprepared-to-deal-with-terror-attack-if-it-happens-pm-lee.

31. Jenkins, Brian Michael. "The Four Defensive Measures Against Terrorism." The RAND Blog. September 24, 2004. http://www.rand.org/blog/2004/09/the-four-defensive-measures-againstterrorism.html.

MAJ Jerry Chua is currently serving as an Officer Commanding in 165 SQN. An Air Warfare Officer (Air Defence Weapons) by vocation, MAJ Jerry Chua was previously a Staff Officer in Capability Development Branch, HQ Air Defence and Operations Command. He holds a Bachelor of Business (Second Class Honours) from NTU. A mid-careerist, MAJ Jerry Chua joined Credit Suisse as an analyst on their graduate programme prior to re-enlisting in the RSAF.

Book Review



Nigel Jones, *Countdown to Valkyrie: The July Plot to Assassinate Hitler, (London: Frontline Books), 2008, 308 pages.*

By **Oliver Cheok**

INTRODUCTION

A common misconception about Germany during World War II (WWII) is that the country was unanimously in support of the fascist Nazi regime. In reality, such a generalisation is not only unfair, but factually untrue as well. One might be surprised to learn that there were over 40 attempts by German resistance to assassinate Adolf Hitler, Führer of Germany, leader of the Nazi political party and dictator of the German Reich.[1]

Of these 40 assassination attempts, none came closer to success than the 20 July Plot, led by Colonel Claus von Stauffenberg. Unfortunately, due to a combination of pure bad luck and human error, the plot was ultimately a failure, and most of its perpetrators executed. Nigel Jones's *Countdown to Valkyrie: The July Plot to Assassinate Hitler* gives a comprehensive account of the events leading up to and the aftermath of the assassination attempt, as well as detailed biographies of all personnel involved.[2]

EARLY LIFE OF COLONEL CLAUS VON STAUFFENBERG

Claus was born on 15th November, 1907, the youngest of four children born to Alfred and Caroline von Stauffenberg. He had two older twin brothers, Alexander and Berthold. Tragically, Claus's own twin brother, Konrad, died shortly after childbirth, on the day of birth.

Born to a wealthy family of nobility, he was afforded a thorough education, but decided to join the military in 1926, against protests from his father. Stauffenberg was likely influenced by his time as a scout as well as his family's rich history in the army. Claus had always been so adamant on joining the army

that in 1914, at the tender age of seven, while Germany was mobilising for war, he cried at the thought that it would be over before he would be old enough to fight. Later on, after serving for 4 years in different regiments and schools, Claus commissioned as a junior officer in 1930.[3]

THE RISE OF HITLER'S NAZIS

Historical texts hint at the idea that even in its infancy, Stauffenberg was not a fan of Nazism. While sympathetic toward its aims of economic reconstruction and rearmament, Claus was purportedly hesitant about its doctrinal discrimination against Jews. Nonetheless, Claus opted to take a wait-and-see attitude toward the Nazi political party in order to cement his allegiance. In addition, Claus had other things on his mind, being promoted to full Lieutenant in 1933 and marrying his wife, Nina von Lerchenfeld, shortly after. [4]

EARLY YEARS OF THE NAZI REGIME

With incredible speed, the Nazi dictatorship took over the entire country. Through a process known as *Gleichschaltung*, all organisations and people were subject to the authority of the new regime. All political parties save the Nazi Socialist German Worker's Party were outlawed. Millions of Germans lived in fear of the German secret police, the *Geheime Staatspolizei* or *Gestapo* for short. [5]

Meanwhile, Claus von Stauffenberg continued to rise through the ranks in the military, during the period Hitler openly declared that Germany was preparing for war, establishing compulsory conscription and allocating resources to the armed forces.

The military restructuring was completed on 4th February, 1938, when Hitler passed a degree appointing himself the supreme commander of the *Wehrmacht*, or German military. Shortly thereafter, the German army began crossing the Austrian border on 12th March, 1938, forcibly taking control. Germany then set her sights on Czechoslovakia.[6]

Hitler subsequently continued his invasion of European territories, taking control of the remainder of Czechoslovakia as well as Poland. Stauffenberg was not alone in his disgust, and resentment against the Nazi regime grew among those in the military. This was perhaps worsened by the fact that Hitler used military force liberally, not affording his soldiers enough time to rest between assaults.[7]

EARLY ATTEMPTS ON HITLER'S LIFE

Resentment against the Führer was so great that the idea of a putsch started to gain traction among *Wehrmacht* officials. This included Army Chief of Staff Halder, who purportedly always carried a pistol when going to see Hitler.[8] However, attempts to act on these conspiratorial thoughts almost always saw plotters getting cold feet.

By 1942, Stauffenberg's allegiance to the Nazi government had all but vanished. He concluded that Germany was on its way to calamity and that it was morally justified to kill Hitler rather than let him remain in power. This was the start of Stauffenberg's involvement in the resistance.

Shortly thereafter, having been posted to North Africa to join the 10th Panzer Division as Operations Officer, Stauffenberg sustained multiple severe wounds when fighter bombers from the Royal Australian Air Force strafed his vehicle. After three months in hospital care, Stauffenberg survived, but lost his left eye, right hand and left hand. He was awarded the Wound Badge in Gold as well as the German Cross.[9]

OPERATION SPARK

Brigadier-General Henning von Tresckow was the chief conspirator in the 20 July Plot, otherwise known as Operation Valkyrie. However, he also spearheaded a number of attempts on Hitler's life prior to the ill-fated plot in question in 1944. Operation Spark is an umbrella term used to refer to these attempts between 1943 and early 1944.

Operation Spark was named after the idea that Hitler's death would provide a 'spark' and trigger the collapse of the Nazi regime. Tresckow believed that while Hitler was alive it would be impossible to overthrow him, by writ of his charisma, numerous successes and the oath of loyalty all Wehrmacht officers had to swear to him.

On a routine visit to *Werwolf*, his field headquarters in Ukraine in February, 1943, Tresckow had arranged with his co-conspirators to smuggle a small explosive in the plane that Hitler was to fly out in. The bomb was smuggled on board disguised as two bottles of Cointreau, an orange-flavored liquor. The bomb was an improvisation of a time bomb created by the British, and consisted of plastic explosives and a pencil detonator.[10]

The detonator contained a copper tube filled with copper chloride. The copper chloride was to take approximately 10 minutes to corrode a wire holding back the bomb's firing pin from its percussion cap. The method of delay was meant to make it stealthier, by avoiding the ticking sound of a clock as well as the smell from a burning fuse. Unfortunately, the method of detonation also ultimately rendered it ineffective due to the cold temperature.

Tresckow arranged for the bomb to be placed on board the plane by his aide, Schlabrendorff. It was to detonate while the plane was near Russian airspace over Minsk, such that it could be attributed to Soviet fighters.

Upon news of Hitler's death, General Friedrich Olbricht was to impose martial law across the country and assume control. This was the precursor to the 20 July Plot, where a similar ploy was planned. However, as fate would have it, the altitude meant that it was too cold for the percussion cap to activate the explosion, and it did not explode. The bomb was later recovered by members of resistance to avoid its discovery. Stauffenberg would later use the same type of bomb in the 20 July attempt on Hitler's life.

EVENTS BEFORE THE 20TH JULY PLOT

After rehabilitating in his home in one of the Stauffenberg castles in southern Germany, Claus was inducted into the team of conspirators and introduced to Tresckow. He was subsequently posted to the *Ersatzheer* where Olbricht was his direct superior.

Olbricht and Stauffenberg recognised that the *Ersatzheer* could be used in a plot to assume control of the Reich. This was because of Operation Valkyrie, a contingency plan which involved imposing martial law over Germany in the event of political turmoil.[11] Operation Valkyrie was meant to ensure that anti-Nazi political parties did not assume control in a political vacuum if the Nazi government were to fall. The conspirators approached Colonel-General Friedrich Fromm, Chief of the *Ersatszheer*, for his support. However, Fromm neither reported them nor agreed to help, instead holding out to see to whom his allegiance would pay the most dividends.[12]

Olbricht believed that the Valkyrie plans could be adjusted such that it would support a coup. This involved spreading a bogus message that Hitler had been assassinated by fellow party leaders, thus activating Operation

Valkyrie to assume control. Between August and September 1943, the conspirators revised the official Valkyrie plans to tailor it to the coup.[13]

Stauffenberg personally went to see the Führer to endorse the amended plan. Hitler signed off without reading the proposal, saying that he was sure it was for the best. The most important factor in the balance was the act of actually killing Hitler, who had thus far managed to evade all attempts on his life. Hitler's paranoia had saved his life on more than one occasion. The only remaining option was another time bomb.[14]

20TH JULY PLOT

On the 14th and 15th of July, Stauffenberg made two more attempts on Hitler's life. On the first day, at a military conference, the plan was aborted because Hitler's right-hand men, Heinrich Himmler and Herman Göring, were not present. It was decided that for the coup to be effective, the entire trio would have to be eliminated. However, with dwindling time, the condition was dropped the next day, and Stauffenberg was to kill Hitler in the *Wolfsschanze*, or Wolf's Lair, Hitler's base.

Once again, fate intervened and the second attempt proved a failure as well. This was because Hitler was called out of the room at the last moment, after the bomb had already been activated and Stauffenberg had made his leave. Stauffenberg was only just barely able to make it back to the room to intercept and defuse the bomb.[15]

The third and final attempt was also to be held in the Wolf's Lair, a week later on 20th July. The attempt was rushed because false rumors had spread that the Gestapo had discovered the plot and were going to arrest the conspirators. Once again, Stauffenberg flew down with the 2-pounds of explosives safely stowed in his briefcase. Upon arrival, Werner von Haefton supplied him with an additional 2-pound explosive. Shortly before the meeting, Stauffenberg excused himself to arm the bombs, saying that that he needed to adjust his bearings.

The subsequent assassination attempt was unsuccessful due to a combination of reasons. Firstly, the meeting's location was changed from an underground bunker to a windowed hut, which would disperse the blast. Time restraints also only allowed Stauffenberg to arm one of the two two-pound bombs. Lastly, a colonel at the meeting accidentally kicked over the briefcase and restored it on the other side of the table leg, made of thick oak. Modern experts agree that if any of these variables had been otherwise Hitler would certainly not have survived. The bomb exploded at exactly 12:42 p.m.[16]

While the meeting was taking place, Stauffenberg took flight with General Erich Fellgiebel, whose job it had been to cut communications from the Wolf's Lair after the detonation. Stauffenberg witnessed the explosion from a distance and assumed Hitler dead. In reality, the table leg had proven thick enough to shield Hitler sufficiently from the blast. Upon landing in Berlin at around 4 pm, Stauffenberg learnt that Hitler had survived the blast and his co-conspirators had not activated Operation Valkyrie due to conflicting information. Olbricht eventually put his foot down and issued orders for Operation Valkyrie to be mobilised. [17]

Subsequently, all over German-occupied territory, members of the Reserve Army were mobilising and taking control, arresting high-ranking government officials. With communications back up, Himmler issued orders to disregard Olbricht's and cease Operation Valkyrie, although the coup was still in full effect in many areas. At around 7 p.m., Hitler had

recovered enough to start making phone calls, and spread the word that he was still alive, quickly putting an end to the coup.[18]

Many of the conspirators had at this point decided to switch sides, and Chief of the Reserve Army Fromm was able to regain control. In order to save himself, and avoid implicit participation in the plot, Fromm quickly ordered executions of all personnel involved, disregarding specific instructions from Hitler to keep all plotters alive. Fromm himself was later found out and sentenced to death as well.[19]

Thus, the closest plot to kill Hitler to ever come to fruition ultimately failed.

CONCLUSION

All things considered, Nigel Jones's book offers the reader a very enjoyable reading experience, and serves as a comprehensive one-book-summary of the German resistance as well as Stauffenberg's life. *Countdown to Valkyrie: The July Plot to Assassinate Hitler* is incredibly readable and comes across more like a narrative rather than a regular old history textbook. The events within its pages are so exciting and nail-biting that it could easily be mistaken for a work of fiction.

The book is also almost completely based on primary sources and is widely considered to be one of the most accurate accounts of the German resistance among experts. I recommend this book to anyone keen on finding out more about Nazi Germany and the realities of living in it.

ENDNOTES

1 Jones, N. (2008). Countdown to Valkyrie: the July plot to assassinate Hitler. Barnsley: Frontline.

2 Ibid., 281.

3 Ibid., 23.

4 Ibid., 27.

5 Ibid., 32.

6 Ibid., 56.

7 Ibid., 80.

8 Ibid., 284.

9 Ibid., 152-155.

10 Ibid., 138.

11 Ibid., 158-159.

12 Ibid., 160-161.

13 Ibid., 199.

14 Ibid., 158-160.

15 Ibid., 180-182.

16 Ibid., 192.

17 Ibid., 201-203.

18 Ibid., 216.

19 Ibid., 283.

Matthew Bunker Ridgway (1895 – 1993)

by **David Ting**

INTRODUCTION

Matthew Bunker Ridgway, also known as Matthew Ridgway was a four-star general from the United States (US) Army, who served from 1917 to 1955. He is most famously known for his contributions during the Korean War (1950-1953), specifically taking over from General Douglas MacArthur after the latter was relieved of duty by President Harry Truman.[1]

EARLY LIFE & CAREER

Matthew Ridgway was born on 3rd March, 1895, at Fort Monroe, Virginia, the son of Thomas Ridgway and Ruth Starbuck Bunker. His father was an artillery colonel who also graduated from West Point in 1883.[2] In addition, his father served in China and during the time of the Boxer Rebellion in 1901. His mother was a concert-class pianist and collector of works of art. [3]

Ridgway graduated from English High School in Boston, Massachusetts in 1912. Being an 'army brat' and wanting to please his father, Ridgway applied to the United States Military Academy (USMA).[4] However, his first attempt was not successful since he failed mathematics. Nevertheless, after much hard work he was admitted in his second application to West Point.[5]

During his time at West Point, Ridgway was the undergraduate manager of the football team. He was classmates with Mark Clark, another revered four-star general from the US Army who served during World War I (WWI), World War II (WWII) and the Korean War.[6] Ridgway's class graduated early in 1917 due to the US engagement in WWI. Ridgway was commissioned as an Infantry officer and rose to Lieutenant in anticipation of joining the war. However, he was posted to Eagle Pass, Texas, where he commanded an Infantry company.

INTERWAR PERIOD

After the war, when General Douglas MacArthur was Superintendent of West Point, he was appointed as an Instructor for Spanish and also an athletic manager.[7] Between 1924 and 1925, Ridgway attended the Company Officers course at Infantry School in Fort Benning, Georgia. Upon graduation, Ridgway was posted to Tientsin, China, where he commanded a company in the 15th Infantry Regiment.[8]

Notably, Ridgway had hoped to be part of the Army's pentathlon team for the 1928 Olympic Summer Games in Amsterdam. But in an interview later, he recalled that "I could not reject so bright an opportunity to prepare myself for any military-diplomatic role that the future might offer."[9] In 1927, persuaded by Major General Frank McCoy, Ridgway was stationed in Nicaragua, where he supervised the 1927 parliamentary election.[10]

Ridgway then went on to graduate from the Army Command and General Staff School at Fort Leavenworth, Kansas in 1935 and the Army War College at Carlisle Barracks, Pennsylvania in 1937.

WORLD WAR II

When the US became involved in WWII, then-Colonel Ridgway was sent to the War Plans Division of the War Department. In January 1942, Ridgway was promoted to Brigadier General and was the commander of the then-82nd Infantry Division. As commander, Ridgway oversaw the training of the unit in North Africa to prepare for the campaign to invade Sicily. In July, the unit arrived in Sicily and soon after on 23rd July, 1943, Prime Minister Benito Mussolini was arrested.[11] Operation Husky, also known as the invasion of Sicily, was a success as the Italian fascist regime fell into the hands of the Allies.

Towards the end of the war, the now veteran 82nd Airborne Division was deployed to the Elsenborn Ridge in Germany to engage in the Battle of the Bulge. They were assigned to take Cheneux where they would force the Waffen SS Division Leibstandarte's Kampfgruppe Peiper into retreat. However, on 24th December, 1944, with a strength of 8,520 men, the 82nd Airborne Division were faced off with a much larger force of 43,000 men. Owing to this circumstance, the division had to withdraw its forces for the first time in its combat history.[12]

The 82nd Airborne Division conducted a counterattack on 3rd January, 1945, and defeated the 62nd Volksgrenadier Division and the 9th SS Panzer Division. However, the counterattack was not without its cost. In the aftermath of the attack, Ridgway lost a Battalion commander, Lieutenant Colonel Joerg, and much of his men were wounded, killed or suffered frostbite.

In March 1945, with the British 6th Airborne Division and the US 17th Airborne Division now under his command, newly promoted Major General Ridgway initiated Operation Varsity and invaded Germany. Subsequently in June 1945, Ridgway was promoted to Lieutenant General and went on to command US troops in Luzon, the Mediterranean and even the Caribbean.

KOREAN WAR

On 22nd December, 1950, Lieutenant General Matthew Ridgway was enjoying a cocktail with his friend when the phone rang. He was informed that General Walton Walker, the commander of the Eight Army, had died in a jeep accident.[13] Ridgway was ordered immediately to fly to Korea and take over General Walker's post. Adding to the confusion, Ridgway was not given any official warning that he was next in line to command the Eight Army.

At this point of time, the Korean War had signified the demise of the American Army. Just five years prior, in 1945, the US were celebrating victory over the Axis Powers. Now, the opposite become reality with Communist Forces chasing American Troops, the vision of a Communist Asia was on the verge of reality and former friends were now formidable adversaries. In a matter of five years, things had changed for America.

For General Ridgway, the challenge was not only unifying the Eight Army but also fixing the strained relations between Washington and the Far East Command.[14] When Ridgway arrived in Korea, he visited the Eight Army which he was to command. To his horror, he discovered that the entire Army was in turmoil. The soldiers lacked proper winter clothing, food was in short supply and the officers would rather flee from the battle.[15] In the days to come, Ridgway learned of rumours that American troops were cheering when they retreated south of the 38th Parallel. Supplies of weapons, ammunition and food were abandoned in the North. This hindered the army from advancing into North Korean territory while expanding the supplies of the communist army.

From his observations, Ridgway concluded that the organisation was lacking competent leaders. This led to a widespread array of problems including a divided army and poorly executed missions, just to name a few. To combat this problem, he restored the soldiers' morale by circulating manifestos that outlined why there were fighting their former allies after the defeat of their once-common enemies and replaced incompetent leaders.[16] Morale immediately went up.

By March, with a revitalised American and South Korean Army, Ridgway not only retook Seoul but managed to get United Nations (UN) forces across the 38th Parallel. A month later, when General Douglas MacArthur was relieved of command by President Harry Truman, Ridgway was finally promoted to General and commander of all UN forces in Korea. General Ridgway would oversee the stalemate of the war until he went to his next post in Europe.

SUPREME ALLIED COMMANDER

In May 1952, General Ridgway took over from General Eisenhower as Supreme Allied Commander Europe (SACEUR). Ridgway was the second general to hold this post.[17] The SACEUR is responsible for Allied Command Operations (ACO) and reports to the Military Committee for military exercises that the North Atlantic Treaty Organisation (NATO) carries out. In addition, the SACEUR is the senior military spokesman for ACO. SACEUR goes for official visits to NATO countries where military operations and countries where NATO is forming alliances with.[18]

During his time as SACEUR, Ridgway developed an effective command structure and improved training and uniformity between the militaries. Furthermore, he supervised an augmentation of the forces. Chairman of the Joint Chief of Staff, General Omar Bradley commented to President Truman that "Ridgway had brought NATO to its realistic phase and a generally encouraging picture of how the heterogeneous defence force is being gradually shaped."[19]

CHIEF OF STAFF, US ARMY

After General Ridgway stepped down from his post as SACEUR in July 1953, he assumed the post of Chief of Staff of the US Army (CSA) from General J. Lawton Collins. This would be his last post before he retired from the military.

Being the most senior officer in the US Army, the CSA directs tasks and ensures co-ordination between service personnel and special staff officers.[20] In addition, the CSA supervises the Army Staff, serves as a member of the Joint Chief of Staff (JCS) and provides military advice to the Secretary of Defence, President and Congress.[21]

During his time as CSA, under the discretion of President Eisenhower, Ridgway was tasked to assess US Military movement in Vietnam in relation to the French. Thus, Ridgway provided Eisenhower with a comprehensive plan that details the crucial actions that will bring success to the US Military. However, President Truman was not keen on the idea. This was because Ridgway's belief in airpower and nuclear bombs did not reduce the size of the need for mobile ground forces to seize land and control communities.[22] Furthermore, Eisenhower's proposal to reduce the size of the army troubled Ridgway because this meant that it would be ill-equipped to counteract the growing force of the Soviet Union.

On the other hand, President Eisenhower approved a waiver that specified that the mandatory military retirement age was 60. This was so that Ridgway could complete his term as CSA. Disagreements between the senior officers and the administration prevented Ridgway from obtaining a second term. He retired from the army on 30th June, 1955, and was succeeded by General Maxwell D. Taylor.

POST-MILITARY LIFE

After his retirement from the military, Ridgway continued to be very active as a speaker, author and leader. He published several books including his war memoirs, titled 'Soldier' and 'The Korean War: How We Met the Challenge'. These books were published in 1956 and 1957 respectively.[23] In addition, Ridgway gave many speeches and participated in various panels, discussions and group.

He also advocated the use of chemical and radiological weapons, arguing that they could protect national interests better than the weapons that the military were currently using.[24]

LEGACY

Ridgway passed away in Fox Chapel, Pennsylvania on 26 July, 1993, at the age of 98 from a heart attack. He is buried at Arlington National Cemetery. In his eulogy, Colin Powell said, "No soldier ever performed his duty better than this man. No soldier ever upheld his honour better than this man. No soldier ever loved his country more than this man did. Every American soldier owes a debt to this great man."[25]

Truly, Powell's statement summarises Ridgway's life as a soldier. He is a remarkable character who held the nation's honour in its highest standard during times of crisis. Certainly, Matthew Ridgway has influenced many young soldiers to achieve their best in the face of adversity.

ENDNOTES

1. Smith, Scott S., Gen. Matthew Ridgway turned the Korean War's tide, *Investor's Business Daily*, https://www.investors.com/news/management/leaders-and-success/matthew-ridgway-turned-the-tide-in-the-korean-war/
2. Arthur, Billy A., Obituary: General Matthew Ridgway, *Independent*, https://www.independent.co.uk/news/people/obituary-general-matthew-ridgway-1460281.html
3. Swanson, Michael D., General Matthew B. Ridgway: Personal Reminiscences by Michael D. Swanson, *The George C.*

Marshall Foundation, https://www.marshallfoundation.org/newsroom/news/general-matthew-b-ridgway-personal-reminiscences-michaeld-swanson-m-d/

The Boxer Rebellion was an uprising during 1899 to 1901 that attempted to drive foreigners out of China.

4. Gen. Matthew B. Ridgway Historical Maker, *Explore PA History*, http://explorepahistory.com/hmarker.php?markerId=1-A-2DF

5. Hickman, Kennedy, Korean War: General Matthew Ridgway, *ThoughtCo*, https://www.thoughtco.com/korean-war-general-matthew-ridgway-2360169

6. Ibid.

7. Swanson, Michael D., General Matthew B. Ridgway: Personal Reminiscences by Michael D. Swanson, *The George C. Marshall Foundation*, https://www.marshallfoundation.org/newsroom/news/general-matthew-b-ridgway-personal-reminiscences-michaeld-swanson-m-d/

8. Matthew Bunker Ridgway, *Arlington National Cemetery*, http://www.arlingtoncemetery.net/ridgway.htm

9. Ridgway, Matthew B., Martin, Harold H., Soldier: The Memiors of Matthew B. Ridgway, *Internet Archive*, https://archive.org/stream/soldierthememoir006996mbp/soldierthememoir006996mbp_djvu.txt

10. Ibid.

11. The 82nd Airborne Division, *Holocaust Encyclopaedia*, https://www.ushmm.org/wlc/en/article.php?ModuleId=10006159

Italian Campaign, *History*, https://www.history.com/topics/world-war-ii/italian-campaign

12. Gavin, James M, *On to Berlin: Battles of an Airborne Commander 1943-1946*, (*Viking*, 1978), 239

13. Hanson, Victor Davis, The Saviour Generals: How Five Commanders Saved Wars That Were Lost-from Ancient Greece to Iraq, (New York City, New York, *Bloomsbury Press*, 2013), 143

14. The Far East Command was based in Tokyo, Japan and it was United States Military Command that lasted from 1947 to 1957.

15. Smith, Scott S., Gen. Matthew Ridgway turned the Korean War's tide, *Investor's Business Daily*, https://www.investors.com/news/management/leaders-and-success/matthew-ridgway-turned-the-tide-in-the-korean-war/https://www.investors.com/news/management/leaders-and-success/matthew-ridgway-turned-the-tide-in-the-korean-war/

16. Hanson, Victor Davis, The Forgotten Maverick General who saved South Korea, *Hoover Institution*, https://www.hoover.org/research/forgotten-maverick-general-who-saved-south-korea

17. Who's who, *North Atlantic Treaty Organisation*, https://www.nato.int/cv/ace-k-p.pdf

18. Ibid.

19. Mitchell, George Charles, "Matthew B. Ridgway: Soldier, Statesmen, Scholar, Citizen", *Stackpole Books*, March 1, 2002, 118.

20. Staff Positions, *Boise State University*, https://sps.boisestate.edu/militaryscience/files/2014/04/Staff-Positions.pdf

Special staff officers are a group officers, both military and civilian personnel who are responsible for the administrative, operational and logical requirements of a unit.

10 US Code 3033 – Chief of Staff, *Legal Information Institute*, https://www.law.cornell.edu/uscode/text/10/3033

21. Mitchell, George Charles. "Matthew B. Ridgway: Soldier, Statesmen, Scholar, Citizen", *Stackpole Books*, March 1, 2002, 143.

22. Matthew Bunker Ridgway, *Encyclopaedia Britannica*, https://www.britannica.com/biography/Matthew-Bunker-Ridgway

23. Mitchell, George Charles, "Matthew B. Ridgway: Soldier, Statesmen, Scholar, Citizen", *Stackpole Books*, March 1, 2002, 143.

24. Ibid, 205.

Quotable Quotes

Long term planning enables us to map out the journey while effective implementation makes sure that we arrive at the planned destination.

-Goh Chok Tong (b. 1941), former Prime Minister and Emeritus Senior Minister of Singapore.

No problem can be solved from the same level of consciousness that created it.

-Albert Einstein (1879-1955), theoretical physicist.

A doctor can only treat patients. A doctor can only help the people who are shot or who are injured. But a politician can stop people from injuries. A politician can take a step so that no person is scared tomorrow.

-Malala Yousafzai (b. 1997), Pakistani activist for female education and the youngest Nobel Prize laureate.

Success is not final, failure is not fatal: it is the courage to continue that counts.

-Winston Churchill (1874-1965), former Prime Minister of the United Kingdom, military officer, historian, writer, artist and Nobel Prize winner in Literature.

Some people dream of success, while other people get up every morning and make it happen.

-Wayne Huizenga (1937-2018), American businessman and entrepreneur.

Battle is the most magnificent competition in which a human being can indulge. It brings out all that is best; it removes all that is base. All men are afraid in battle. The coward is the one who lets his fear overcome his sense of duty. Duty is the essence of manhood.

-George S. Patton (1895-1945), United States Army General

Peace is not absence of conflict, it is the ability to handle conflict by peaceful means.

-Ronald Reagan (1911-2004), 40th President of the United States

Twenty years from now you will be more disappointed by the things that you didn't do than by the ones you did do.

-Mark Twain (1835-1910), American writer

If civilization is to survive, we must cultivate the science of human relationships - the ability of all people, of all kinds, to live together, in the same world of peace.

-Franklin D. Roosevelt (1882-1945), 32nd President of the United States

Your work is going to fill a large part of your life, and the only way to be truly satisfied is to do what you believe is great work. And the only way to do great work is to love what you do. If you haven't found it yet, keep looking. Don't settle. As with all matters of the heart, you'll know when you find it.

-Steve Jobs (1955-2011), Co-Founder, Chairman and CEO of Apple.Inc, entrepreneur, marketer, inventor.

Adopt the pace of nature: her secret is patience.
-Ralph Waldo Emerson (1803-1882), American Poet

We are made wise not by the recollection of our past, but by the responsibility for our future.
-George Bernard Shaw (1856-1950), Irish Playwright

The pessimist complains about the wind; the optimist expects it to change; the realist adjusts the sails.
-William Arthur Ward (1921-1994), American Writer

True knowledge exists in knowing that you know nothing.
-Socrates (469-399 BC), Greek Philosopher

By three methods we may learn wisdom: First, by reflection, which is noblest; Second, by imitation, which is easiest; and third by experience, which is the bitterest.
-Confucius (551-479 BC), Chinese Philosopher

The greater danger for most of us lies not in setting our aim too high and falling short; but in setting our aim too low, and achieving our mark.
-Michelangelo (1475-1564), Italian sculptor, painter, architect and poet

Knowledge comes, but wisdom lingers. It may not be difficult to store up in the mind a vast quantity of facts within a comparatively short time, but the ability to form judgments requires the severe discipline of hard work and the tempering heat of experience and maturity.
-Calvin Coolidge (1872-1933), 30th President of the United States

The best and most beautiful things in the world cannot be seen or even touched.
They must be felt with the heart.
-Helen Keller (1880-1986), American author, political activist, and lecturer

The lessons from the peace process are clear; whatever life throws at us, our individual responses will be all the stronger for working together and sharing the load.
-Queen Elizabeth II (b.1926), Queen of the United Kingdom and the other Commonwealth realms

A good head and a good heart are always a formidable combination.
-Nelson Mandela (1918-2013), South African anti-apartheid revolutionary,
political leader, peace activist, and philanthropist

Leadership is solving problems. The day soldiers stop bringing you their problems is the day you have stopped leading them. They have either lost confidence that you can help or concluded you do not care.
Either case is a failure of leadership.
-Colin Powell (b. 1937), American statesman and a retired four-star general

Chief of Defence Force Essay Competition 2017/2018
Prize Winners

FIRST PRIZE

Tackling the Returning Foreign Fighter Threat: Hard or Soft Approach
LTC Harris Tan Nan An

SECOND PRIZE

Accelerating the 4th Industrial Revolution in the SAF
ME4 Albany Loh & CPT Lee Zi Yang

THIRD PRIZE (TIED)

The Rise of the Fifth Domain and its Legal Considerations
CPT Cristal-Anne Low Jie Xin

Seven Paradoxes: Challenges for the Next Gen SAF
LTC Chong Shi Hao

MERIT AWARDS

Regulating Cyberspace: Singapore's Place in the Global Conversation on Cyber Norms
CPT Matthias Chia Boon Liang & CPT Chris-Adelle Khaw Jing Rui

Edge Computing: Optimising Training through Data Analytics
MAJ Alvin Quek

Intelligence in a New Age of War
CPT Katie Qintan Lin

Submerged Ambitions – Emerging Challenges and Opportunities for Managing Submarine Proliferation in East Asian Waters
MAJ Benson Chian

Developing the Bases of Powers as a Leader – A Comparison of Two Great Military Leaders
MAJ Timothy Koh Tong Choon

A Nudge for the Military
ME6 Calvin Seah Ser Thong

COMMENDATION AWARDS

The Age of Ultron: Implications of Malicious Artificial Intelligence for Information Warfare and Cyber Security
CPT Tan Rui Lin, CPT Thia Shan Zhi & CPT Zech Tan E-An

Fighting Fire with Fire – Using Hybrid Solutions against a Hybrid Enemy
MAJ Ho Jin Peng

To What Extent Do Militaries Need to Do Operations Other Than War?
MAJ Stanley Lim

Maritime Sense-making and the Role of Big Data Analytics for Enhancing Maritime Security
COL Nicholas Lim & LTA Chong De Xian

Hanging by a Thread – Our Connection to War
ME6 Calvin Seah Ser Thong

Sweat Hard, Not Blood – Leadership Models for Realistic and Safe Military Training
LTC(NS) Denzil Titt

Overcoming the SAF's Challenges using the 4th Industrial Revolution Technology
ME5 Ong Wen Xiang

Effectiveness of Singapore's Defence and Foreign Policies for Achieving its National Interests
MAJ Leow Yew Hock

A Costless War through Armed Unmanned and Robotic Systems
MAJ Lim Chong Siong

Security Challenges and Opportunities of 4th Industrial Revolution
CPT Foo Sze Wei

Organisational Culture's Effect on leadership – A USAF UAV Perspective
MAJ Joe Ee Pinn Hwee

Instructions for Authors

AIMS & SCOPE

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

SUBMISSION DEADLINES

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

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

SUBMISSION GUIDELINES

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

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

Article Topics

POINTER accepts contributions on the following topics:

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

Book Reviews

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

Viewpoints

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

Required Information

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

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

Submission of Manuscript

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

Article Length

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

ENDNOTE FORMAT

Author's Responsibilities

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

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

Endnotes

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

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

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

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

Books

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

For example:

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

Huxley, *Defending the Lion City,* 4.

Ibid., 4.

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

Articles in Periodicals

Citations should include the author, title of the article (quotation marks), title of periodical (italicised), issue information (volume, issue number, date of

publication), appropriate page reference, and URL in the case of e-books. Note that the volume number immediately follows the italicised title without intervening punctuation, and that page reference is preceded by a colon in the full citation and a comma in abbreviated citations.

For example:

Chan Kim Yin and Psalm Lew, "The Challenge of Systematic Leadership Development in the SAF," *POINTER* 30, no. 4 (2005): 39-50.

Chan and Lew, "The Challenge of Systematic Leadership Development in the SAF," 39-50.

Ibid., 39-50.

Mark J. Valencia, "Regional Maritime Regime Building: Prospects in Northeast and Southeast Asia," *Ocean Development and International Law* 31 (2000): 241.

Articles in Books or Compiled Works

Michael I. Handel, "Introduction," in *Clausewitz and Modern Strategy,* ed. Michael I. Handel, (London: Frank Cass, 1986), 3.

H. Rothfels, "Clausewitz," in *Makers of Modern Strategy: Military thought from Machiavelli to Hitler,* eds. Edward Mead Earle and Brian Roy, (Princeton: Princeton University Press, 1971), 102.

Articles in Newspapers

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

For example:

David Boey, "Old Soldiers Still Have Something to Teach," *The Straits Times,* 28 September 2004, 12.

Donald Urquhart, "US Leaves it to Littoral States; Admiral Fallon Says Region Can Do Adequate Job in Securing Straits," *The Business Times Singapore,* 2 April 2004, 10.

Online Sources

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

For example:

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

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

For example:

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

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

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

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

EDITORIAL ADDRESS

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

COPYRIGHT

REPRINTS

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

PLAGIARISM

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

POINTER

The Journal of the Singapore Armed Forces

ISSN 2017-3956