POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

Vol. 43 No. 1 [2017]

Editorial Board

The opinions and views expressed in this journal do not necessarily reflect the official views of the Ministry of Defence. The Editorial Board reserves the right to edit and publish selected articles according to its editorial requirements. Copyright© 2017 by the Government of the Republic of Singapore. All rights reserved. The articles in this journal are not to be reproduced in part or in whole without the consent of the Ministry of Defence.

POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

ISSN 2017-3956 Vol. 43 No. 1 [2017]

contents

FEATURES

contents

BOOK REVIEW

PERSONALITY PROFILE

QUOTABLE QUOTES

Editorial

In this first issue of POINTER for 2017, we are pleased to present an Air Force-themed issue. The theme is 'Dealing with the Challenges of Hybrid Warfare: An RSAF Perspective.' Today, threats and challenges to Singapore may come in many unexpected shapes and forms. The nature of warfare is also evolving. It will become more complex and can involve weakening the target nation through non-kinetic means such as cyber attacks and generating social tension through disinformation. Such campaigns, blending conventional warfare with elements of irregular warfare and non-kinetic attacks, are commonly referred to as hybrid warfare. The essays in this issue will explore important topics that the Republic of Singapore Air Force (RSAF) needs to reflect upon, in the face of hybrid warfare, covering possible changes in their operating context, challenges and opportunities that they will encounter, and the capacity and new competencies that they need to create within the RSAF.

The essay entitled, 'Against the Ascent of Hybrid Warfare: Expanding the RSAF's Capacity in Peace and War' is by SLTC Wong Hin Kai, MAJ Anthony Lau Kai Heng and CPT James Yong Dun Jie. In this essay, the authors define the concept of hybrid warfare and examines what this means to Singapore and the RSAF. The authors highlight that the RSAF is a highly responsive force, capable of handling a wide spectrum of missions from peace to war. According to them, while the ability to deal with conventional warfare remains RSAF's *raison d'etre*, the RSAF will increasingly be called upon to address threats and contingencies in peacetime. This is a consequence of rising global interdependency and interconnectivity, where the application of hybrid warfare by state and non-state actors through a blend of conventional and unconventional, regular and irregular, as well as information and cyber means becomes more prevalent. Singapore, given our connectivity to the world, geostrategic locale and demographic makeup, is not immune to these multi-faceted threats that are without clearly-defined adversaries and time frames. The authors conclude that to sustain Singapore's peace and security, the RSAF must remain relevant and effective as it contributes to the Whole-Of-Government approach in countering potential hybrid threats.

The essay, 'Technologies in Hybrid Warfare: Challenges and Opportunities' is written by ME6 Gabriel Tham, CPT Edward Wong & ME4 Kelvin Kuo Kai Ming and discusses how emerging and disruptive technologies may be harnessed to overcome challenges posed by hybrid warfare and the potential pitfalls that may be introduced by such technologies. The authors stressed that in recent years, hybrid warfare has become increasingly wide spread, comprising various conventional and non-conventional means of warfare, as well as non-military options. They highlighted that while technological progress would generate more opportunities, it could also bring about threats to a country. They have cited examples such as drone-related technologies which could pose a sizeable threat due to their accessibility and low cost, enabling mass production and swarm tactics. For Singapore, the RSAF will also have to consider methods of minimising collateral damage in air strikes, to alert civilians to impending air strikes, although such technologies are not without limitations. The authors added that Electromagnetic Pulse (EMP) weapons could also pose a significant threat to Singapore, and to combat these, the RSAF could choose to employ active or passive systems. The authors conclude that ultimately, continual technological development is essential for the RSAF to maintain its edge over potential aggressors.

LTC Anthony Wong, MAJ Christopher Eng, CPT Ronald Loh Ming Yao and CPT Jeffrey Ng present their perspective on 'Cyber Threats in Hybrid Warfare: Securing Cyberspace for the RSAF'. Their essay explores cyber security in the light of the ascent of hybrid warfare and its implications for the RSAF. This essay focuses on how cyber attacks have evolved over the years and how other established militaries addressed the cyber threat challenge. Drawing insights from these observations and in the face of an increasingly sophisticated cyber threat environment, the authors highlighted that the RSAF would need to develop a multi-layered cyber defence strategy to guard its capabilities and operational effectiveness in peace and war.

The fourth essay, 'Developing Key Competencies in the RSAF to Defend Against Hybrid Warfare' by ME6 Spencer Goh, MAJ Joe Zhang, MAJ Tang Mun Bbun and CPT Rae Tan Yiwei examines the attributes and skillsets that are required of RSAF professionals in order for the RSAF to remain responsive to the threat of hybrid warfare. According to the authors, Singapore is a small country with open and intricate technological networks and as such, we are particularly susceptible to hybrid wars where military and non-military tools are employed in an integrated campaign to achieve surprise, seize the initiative and overcome a country. In order to protect Singapore, the authors feel that the Singapore Armed Forces (SAF) should increase its focus on building the capabilities to counter the unconventional threats that are typically used in hybrid warfare. Their essay focuses on the four typical domains within hybrid warfare namely, information, cyber, electronic and intelligence. The authors feel that these are the areas in which the RSAF must build on, in order to be able to defend Singapore by ensuring the attainment of air superiority and the provision of support for the SAF and Whole-of-Government efforts in hybrid warfare.

The final essay, 'NS50: Defending Singapore 50 Years and Beyond' by LTC Low Teck Loong, LTC Lee Kok Kiang, MAJ Nah Jinping and CPT Aaron Chan reflects on the success of National Service (NS) over the past 50 years as well as explores further avenues to encourage Singaporeans to take greater ownership of keeping Singapore safe, strong and resilient in the face of all forms of threats through NS. In commemoration of the 50th anniversary of NS this year, the essay briefly traces the origins of NS as a necessary response to the critical need of national security in newly-independent Singapore. The authors highlight that part of the success of the policy has been due to its evolution over the years to stay relevant to Singapore's society and meet our security needs. This has included building a strong NS training system, creating the Singapore Armed Forces Volunteer Corps (SAFVC), increasing opportunities for National Servicemen (NSmen) to contribute, easing administrative restrictions, improving recognition and benefits for NSmen and encouraging community support for them. Lastly, the authors considered several possibilities of how the RSAF could tap on the NS resources in response to emerging threats in hybrid warfare, such as harnessing the current force and shaping the future, strengthening individual skills and knowledge and strengthening partnership with the private sector and other ministries.

At this juncture, POINTER would like to bid a fond farewell to LCP Jeria Kua as he leaves to pursue further studies. We thank him for his contributions and wish him well in his future endeavours.

A warm welcome to Mr Josiah Liang, our DPO representative who joins the POINTER Editorial Board.

We would also like to extend our warmest welcome to COL Simon Lee who takes over as Chairman, POINTER Editorial Board. Welcome, Sir!

The POINTER Editorial Team

Against the Ascent of Hybrid Warfare: Expanding the RSAF's Capacity in Peace and War

by SLTC Wong Hin Kai, MAJ Anthony Lau Kai Heng & CPT James Yong Dun Jie

Abstract:

The authors highlight that the RSAF is a highly responsive force, capable of handling a wide spectrum of missions from peace to war. According to them, while our ability to deal with conventional warfare remains our *raison d'etre*, the RSAF will increasingly be called upon to address threats and contingencies in peacetime. This is a consequence of rising global interdependency and interconnectivity, where the application of hybrid warfare by state and non-state actors through a blend of conventional and unconventional, regular and irregular, as well as information and cyber means becomes more prevalent. Singapore, given our connectivity to the world, geostrategic locale and demographic makeup, is not immune to these multi-faceted threats that are without clearly-defined adversaries and time frames. To sustain Singapore's peace and security, the RSAF must remain relevant and effective as it contributes to the Whole-Of-Government approach in countering potential hybrid threats.

Keywords: Hybrid Warfare, Technology, Human Capital, Homeland Security, Resilience

INTRODUCTION

The Republic of Singapore Air Force (RSAF) is a highly responsive force, capable of handling a wide spectrum of missions from peace to war. While our ability to deal with conventional warfare remains our *raison d'etre*, the RSAF will increasingly be called upon to address threats and contingencies in peacetime. This is a consequence of rising global interdependency and interconnectivity, where the application of hybrid warfare by state and non-state actors through a blend of conventional and unconventional, regular and irregular, as well as information and cyber means becomes more prevalent. Singapore, given our connectivity to the world, geostrategic locale and demographic makeup, is not immune to these multi-faceted threats that are without clearly-defined adversaries and time frames. To sustain Singapore's peace and security, the RSAF must remain relevant and effective as it contributes to the Whole-Of-Government approach in countering potential hybrid threats.

This essay will outline the ascent of hybrid warfare and the associated threats to states, along with how the RSAF is currently contributing to Singapore's defence against this emerging form of warfare. The essay will conclude with the proposition for the RSAF to continue to sharpen and strengthen its edge against hybrid threats, by actively exploring new opportunities and further developing our people and capabilities.

HYBRID WARFARE

> *"The very 'rules of war' have changed. 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. The focus of applied methods of conflict has altered in the direction of the*

> *broad use of political, economic, informational, humanitarian and other non-military measures—applied in co-ordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict."*
>
> *- General Valery Gerasimov, 2013*[1]

According to the 'Gerasimov Doctrine', hybrid warfare comprises three mutually-reinforcing principles. First, it blurs the boundaries between wartime and peacetime, space and time, as well as the actors involved. This makes it increasingly difficult for one to assess if a state is at war, under attack or at peace, and targeted by whom. Second, it involves the combined use of instruments of national power to achieve the desired end state. Military forces are no longer just applied in conventional warfare but have become a part of the broader national strategy. Third, it involves the simultaneous and co-ordinated application of instruments of national power, making it extremely challenging for a state to detect the centre of gravity of the attack and consequently its ability to counter the attack.[2]

The Changing Face of Modern Warfare

The concept of hybrid warfare is not new. In 1999, two senior officers from the People's Liberation Army published a book on how a nation can defeat a technologically superior opponent through alternative methods such as 'Lawfare', Economic and Network warfare, and Terrorism.[3] In the past decade, the application of hybrid warfare has been gaining ground where different instruments of national power were purposefully co-ordinated and employed by adversarial states to achieve their strategic objectives. Notable

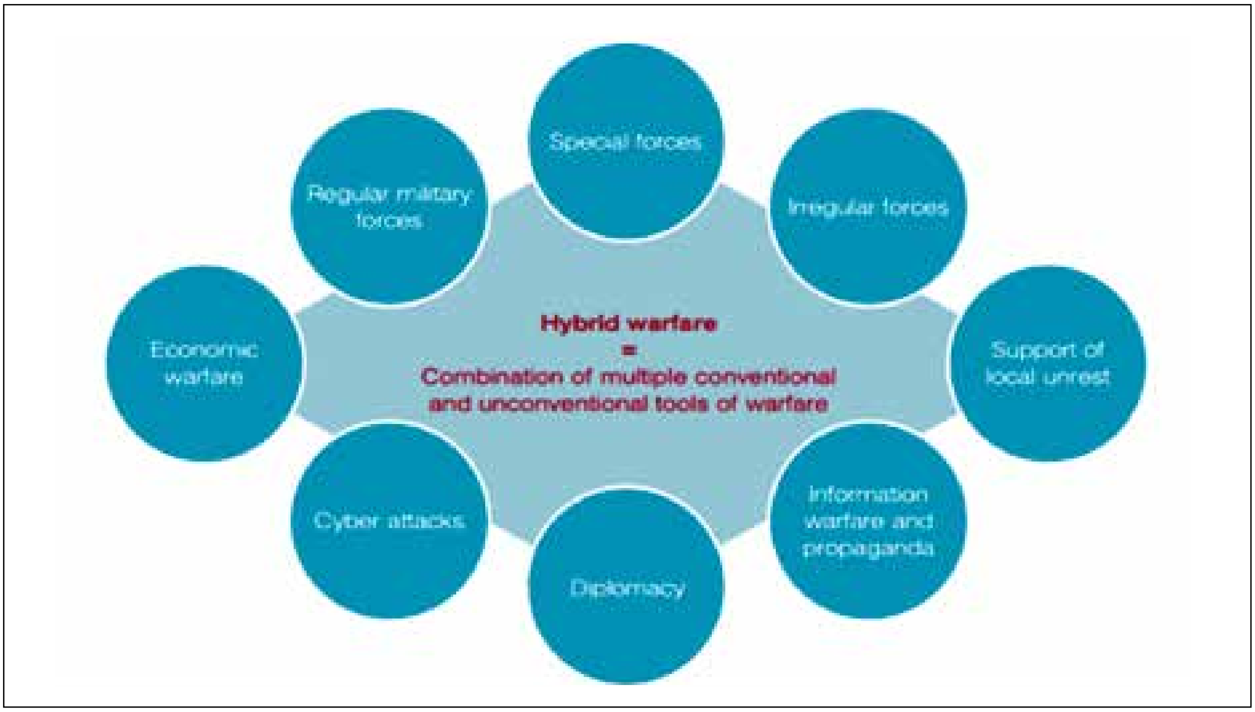

Special forces
Regular military forces
Irregular forces
Economic warfare
Hybrid warfare = Combination of multiple conventional and unconventional tools of warfare
Support of local unrest
Cyber attacks
Information warfare and propaganda
Diplomacy

Figure 1: Concept of Hybrid Warfare[4]

examples include the 2nd Lebanon War in 2006, the Estonian Cyberwar in 2007, the Russo-Georgian War in 2008 and most recently, the on-going hybrid war against the Islamic State of Iraq and Syria (ISIS). Specifically, Russia's operations in Crimea and subsequently in Eastern Ukraine have shown a growing emphasis on 'guerrilla geopolitics' in which novel tactics are needed to target enemy weaknesses and avoid overt altercations, especially with powers or alliances with greater military, political and economic might.[5]

The Ascent of Hybrid Warfare

As states become increasingly connected and dependent on one another, the 'cost' of a full-scale conventional war becomes a less attractive tool or option to be considered for the resolution of conflicts. The Trans-Pacific Partnership, Regional Comprehensive Economic Partnership as well as the Association of Southeast Asian Nation (ASEAN) Plus Free Trade Agreements, which serve as building blocks towards greater regional economic integration and an eventual Free Trade Area of the Asia Pacific, are just some examples of how global interdependencies have significantly reduced the odds of a direct military confrontation between rivals today.

Besides the plausible blending of national powers to threaten a state from multiple fronts—terror, cyber, information, psychological, conventional and criminal—the fact that such threats are more challenging to detect and counter as opposed to dealing with a direct adversary in conventional warfare has made hybrid warfare a more attractive option for states in achieving their strategic objectives.[6]

Moreover, it maximises the likelihood of survival and even victory for a state that is up against another that is superior in numbers, tactics and technology.[7] For instance, the on-going territorial disputes in the East and South China Seas may provide an ideal test bed for states to employ hybrid warfare and allow them to potentially gain an advantage unnoticed. While a 'war' in such a contested space may already have taken place psychologically, politically and economically even though conventional forces are not employed, it will be so subtle, incremental and abstruse that the states concerned may either not know that they are being challenged, or are unable to respond adequately as they have realised the situation too late.[8]

Beyond state-on-state conflicts, hybrid warfare may also be pursued by non-state actors where irregular procedures and tactics are employed against states. Such unconventional methods may range from terrorism, insurgency, guerrilla fights, organised crime, cyber attacks against military targets and financial institutions, as well as the destruction of essential infrastructure, communications and transport elements.[9] This is perhaps best illustrated by the on-going conflict with ISIS.

As states become increasingly connected and dependent on one another, the 'cost' of a full-scale conventional war becomes a less attractive tool or option to be considered for the resolution of conflicts

Hybrid Threats

Hybrid threats can adopt and adapt a wide range of technology, including weapons of mass destruction. Such threats can operate conventionally and unconventionally, and employ asymmetric permutations of traditional, irregular and criminal manoeuvres in a flexible manner.[10] Beyond the use of the military instrument, other instruments of national power—diplomatic, economic and information—

are also exploited in the hybrid threat construct to exacerbate an already complex problem for states.

On the diplomatic front, international organisations or forums have and will continue to serve as platforms for states to garner support for their strategic agendas, and to justify *jus ad bellum* during conflicts with their adversaries. In our region, forums such as the ASEAN Defence Ministers' Meeting (ADMM) and the ADMM-Plus have performed fairly well as avenues to discuss and exchange views on Southeast Asian security issues as well as to promote practical functional co-operation.[11] However, the seemingly inevitable shift from the current United States (US) unipolarism to a bi-polar or multi-polar international system will require smaller states to be more dexterous in their use of diplomacy.[12] In particular, it remains to be seen if the influence of existing international organisations and forums will be diluted due to the rise of new partnerships such as those fronted by China. This may eventually compel some states to consider employing non-state actors for non-attributable but impactful influences on their adversaries, adding new complexities to the nature of conflicts. Given the digitisation and interconnectivity across financial markets, states could leverage economic levers—forceful fiscal policies, currency intervention or even trade sanctions—to indirectly reduce another state's political and military influences. States could also exploit trade interdependencies to manipulate or even immobilise their adversary's key imports and exports, with the aim of stifling their economy.

The future technology landscape will be replete with innovations that will underpin developments in the military and information domains of hybrid warfare. The growing ubiquity of high-speed Internet access, proliferation of mobile devices and the advent of the 'Internet of Things' will see cyber space becoming not only an intrinsic part of peoples' lives, but also a strategic integrator of armed forces and military technology.[13] Space-based technologies and artificial intelligence will scale new heights, and these will very much empower individuals and improve lives at the same time. However, the rapid pace of technological advances also presents a host of new threats to national security in the military and information domains, as the nature of conflict assumes a new complexion with state and non-state actors seeking to exploit them for their pugnacious objectives.

Singapore is certainly not immune to hybrid threats. As a 'little red dot' with an open economy that is subject to varying influences, Singapore is particularly susceptible to hybrid warfare. Considering reports of Russia's successful 'demonstration' of the effective use of non-kinetic options such as cyber attacks, information warfare and propaganda in Crimea and Eastern Ukraine, Singapore's extensive reliance on technology, networks and connectivity has provided the requisite infrastructure for these non-kinetic options to thrive in. It is therefore critical that Singapore, the Singapore Armed Forces (SAF) and the RSAF continue to build up a strong defence during peace, and further leverage new technologies to respond to security challenges externally and internally.

The future technology landscape will be replete with innovations that will underpin developments in the military and information domains of hybrid warfare.

THE RSAF'S CONTRIBUTIONS TO SINGAPORE'S DEFENCE AGAINST HYBRID WARFARE

The SAF's primary role is to enhance Singapore's peace and security through deterrence and diplomacy, and should these fail, to secure a swift and decisive

In 2010, the Heron 1 Unmanned Aerial Vehicle (UAV) took over the Searcher-class UAV, which had been in service with the RSAF since 1994.

victory over the aggressor. A strong SAF forms the bedrock for a peaceful, stable country that creates conditions conducive for economic growth and the well-being of its people. However, should war break out, the nation depends on the SAF to defeat the aggressors swiftly and decisively. In this regard, the RSAF plays an important role in the overall SAF campaign through its provision of Air Power with speed, reach, flexibility, precision and mobility.

SHAPING THE SAF'S CAMPAIGN DECISIVELY, PROVIDING SUPPORT FOR HOMELAND SECURITY

In conventional warfare, amongst many other functions, the RSAF is capable of decisively shaping the SAF's campaign by (1) pursuing air superiority so as to ensure the freedom of movement for the SAF's ground and naval forces; (2) neutralising strategic targets with the firepower of its high-end fighters and attack helicopters; and (3) increasing the success rate for upcoming missions through the use of its airborne surveillance and reconnaissance capabilities, which include the Unmanned Aerial Vehicles (UAVs). The RSAF offers the SAF a strategic leverage with its strong air combat assets that can be deployed to either neutralise dangerous threats posed by the adversary before the deployment of ground troops, serve as a deterrence against enemy troops, or offer vital protection for our military forces when required.

In hybrid warfare, adversaries may also deploy irregular forces such as civilian-dressed individuals to damage civil infrastructure or harm the population directly through the use of terrorist methods. This will undermine the government's ability to provide basic security for the nation's larger nation-building efforts, and weaken the population's confidence and will to fight. It is thus important for the RSAF to continue to lean forward in support of the SAF and other national security agencies for homeland security, even as it commits itself to winning the military campaign.

The RSAF's UAV assets can provide tremendous value in this regard. The UAVs are able to provide pervasive surveillance over large areas and pick up real-time imagery of suspicious activities. This facilitates the co-ordination of the necessary responses to quell threats posed by irregular forces promptly. The usefulness of the RSAF's UAV assets in protecting civil infrastructure and the population can be seen in the success of the deployment of a UAV Task Group to Afghanistan in 2010. In this deployment, the UAV Task Group supported the multinational reconstruction efforts in Afghanistan by providing surveillance over key roads and identifying Improvised Explosive Devices (IED) threats. These enhanced the security of Afghan locals and international forces there.[14] The lessons learned and skills honed could also be employed in enhancing our homeland security.

STAYING VIGILANT AT HOME, CONTRIBUTING TO THE INTERNATIONAL FIGHT AGAINST TERRORISM

During peacetime, the RSAF also plays highly important roles in protecting Singapore's skies and

Wikipedia/Luhai Wong

RSAF pilots dashing to their fighter jets after being activated.

advancing Singapore's interests. With terrorism, threats can come in unexpected ways, suddenly, and from anywhere. Such threats seek to strike fear in the populace whether by directly imposing harm to their lives or by affecting the economy. The 9/11 incident, which saw terrorists hijack four civil airliners and crashing three of them into the Twin Towers in Manhattan and the Pentagon in Arlington County, was a grim example of such a devastating threat. The RSAF is deeply aware of the devastation such aerial threats can pose to the nation, and stays vigilant 24/7 to guard against these types of attacks. In safeguarding the peace and security of Singapore, the RSAF monitors Singapore's skies round the clock with its robust suite of sensors and information networks to identify and track potential threats. If necessary, at any point in time, the air defence control team on duty can orchestrate a rapid response by activating the RSAF's fighter jets and Ground-Based Air Defence (GBAD) units on 24/7 standby.[15] Such a contingency occurred in 2008 when the RSAF activated two F-16 fighters to intercept a Cessna 208 aircraft that was flying towards Singapore airspace without an approved flight plan.[16]

The emergence of extremism and terrorist attacks which target civilian populations appears to be a long-term threat which may form a 'new normal of troubled peace'. In a speech at the 15th Shangri-La Dialogue, Minister for Defence Dr. Ng Eng Hen highlighted a need for countries and their security forces to work closely together to combat terrorism, besides strengthening national security. In a separate speech, he also acknowledged that the threat posed by terrorism is a long-term one, and "unless the source of this radicalisation is disrupted, our citizens at home cannot be protected".[17] This was why Singapore decided to deploy military assets to support the multinational efforts in tackling the ISIS threat at its source.[18]

Capabilities provided by the RSAF have proven to be highly relevant in supporting this cause. For example, the deployment of an Imagery Analysis Team (IAT) at the Combined Joint Task Force Headquarters in Kuwait since September 2015 provided the coalition with intelligence support to identify terrorist infrastructure and activities.[19] The RSAF also deployed a KC-135R tanker to support the air-to-air refuelling of coalition aircraft in May 2015. These contributions offered valuable help and were appreciated by international partners.

CONTRIBUTING TO SINGAPORE'S TOTAL DEFENCE

The 'new normal of troubled peace' that Singapore could face will contain multiple characteristics of hybrid warfare—a blurring of distinction between peace and war, increased attacks on non-kinetic domains such as cyber space and the informational sphere, and the unclear attribution of perpetrators. Affirmed in a speech by Minister for Defence Dr. Ng Eng Hen at the Committee of Supply Debate 2015, the Total Defence concept continues to be the way forward to counter hybrid warfare and sustain a resilient Singaporean society.[20]

The RSAF plays important roles in the pillars of Total Defence. Of significance, the RSAF, widely recognised as a technologically advanced and professional air force, contributed directly to the SAF's ability in maintaining an effective deterrence against potential aggressors, and countering other peacetime threats. The RSAF also keeps up its contributions to Military Defence by continually renewing its technology to sustain its technological lead, and regularly honing its warfighting capabilities through recurring overseas exercises such as Forging Sabre, Cope Tiger and Wallaby. For Civil Defence, the RSAF's multiple contributions to Humanitarian Assistance and Disaster Relief (HADR) efforts over the years not only showed that the RSAF has relevant capabilities to contribute to swift and effective disaster relief, but also strengthened the nation's capability in handling the aftermath of a crisis. Examples of the RSAF's deployments include aiding Indonesia in its rescue efforts in the aftermath of the Boxing Day tsunami in 2004, participating in the search-and-recovery efforts for downed AirAsia flight QZ8501 in 2014, and assisting in firefighting efforts in Chiang Mai in 2015. The profiling of the RSAF's strong capabilities, high operational readiness, and mission success also lends support to Psychological Defence. A strong and effective RSAF helps to strengthen the public's confidence and positive perception of Singapore's defence, and reaffirm the strength of our nation.

MINDEF

RSAF aircraft being deployed to Indonesia to assist in the first phase of disaster relief operations in the wake of the Boxing Day tsunami in 2004.

To remain relevant and prepared, the RSAF has to constantly review the effectiveness of our platforms and systems against hybrid threats and exploit opportunities presented by technology.

EXPANDING THE RSAF'S CAPACITY IN PEACE AND WAR

The RSAF of the future must continue to sharpen and strengthen its edge against the threat of hybrid warfare. It must actively seek out new opportunities and explore novel capability domains afforded by advancements in technology, build safeguards and review our concept of operations in the face of mounting threats in cyber space, develop our people to operate certain critical capabilities and better respond against hybrid warfare, and further strengthen our National Service (NS) construct and resilience against the dangerous hybrid threats in an increasingly complex and contested environment.

Harnessing Advancements In Technology

Technological advances and greater connectivity have and will continue to influence the speed and lethality of hybrid warfare as well as the manner in which it is conducted. To remain relevant and prepared, the RSAF has to constantly review the effectiveness of our platforms and systems against hybrid threats and exploit opportunities presented by technology. While technology will continue to be a critical force multiplier for a small Air Force such as ours, the RSAF must also be cognisant of the potential pitfalls that may be brought forth through their application. The RSAF will do well to develop the necessary defences against these, taking into consideration our unique context and constraints.

Building Strong Cyber Defence

As the RSAF becomes increasingly networked in the years ahead, its growing reliance on cyber space to integrate technologies and forces will pose challenges. To guard against degradation of the RSAF's capabilities and operational effectiveness in peace and war, we must build up our cyber defence capacity and re-examine whether existing concepts of operations are still optimal in employing airpower during cyber attacks. Given the emphasis on cyber defence developments in the SAF, the RSAF must continue to learn and gain insights from other established militaries on how they are addressing cyber-related challenges in hybrid warfare. The RSAF should also further explore and develop new concepts of conducting cyber defence, in order to ensure the effective employment of our warfighting capabilities even in the face of an increasingly sophisticated cyber threat environment.

Developing The RSAF's Human Capital

Fuelled by rapidly-developing technologies, the proliferation of hybrid threats will require certain critical capabilities and competencies in Information-Cyber-Electronic-Intelligence domains to be developed for an effective defence. This brings about new human capital demands beyond the already high commitments for the RSAF's conventional military capabilities. The RSAF will need to raise, train and sustain the requisite manpower and build up the right competencies in them to operate such capabilities effectively. Amidst the backdrop of Singapore's population challenges, however, it is essential for the RSAF to examine the relevance of our current vocational expertise in taking on the new roles while considering new vocations we might possibly need.

Enhancing Resilience Through NS

The concept of NS has served Singapore well over the past fifty years. As we celebrate NS50, it is important for the RSAF to reaffirm the role and contributions of our NSmen and examine how the current NS construct can be further sharpened and strengthened to support the national effort against hybrid threats. Specifically, the RSAF will need to look at better engaging our NSmen to keep them abreast with the latest developments in our threat environment, as well as examine how they can better work together with their active counterparts and support capabilities in response to the persistent but evolving security challenges. Beyond military capacities, the RSAF will also need to explore other avenues that will better leverage NS to encourage Singaporeans to take greater ownership in keeping Singapore safe, strong and resilient.

CONCLUSION

In conventional capability, the RSAF has done well in attaining a significant edge in direct conflicts. Instead of a head-on confrontation with us, potential adversaries are likely to employ hybrid warfare and try to wear us down with protracted low-intensity conflicts below the threshold of war. To continue to safeguard Singapore's peace and security, the RSAF will need to expand capacity in both peace and war. Moving forward, the RSAF should look at developing effective non-conventional capabilities to complement our conventional build-up under the 3rd Generation RSAF transformation. The essays in this journal will outline some key thrusts that the RSAF could explore in order to remain relevant and effective against the ever-evolving threat of hybrid warfare in an uncertain world.

ENDNOTES

1. V. Gerasimov, The Value of Science in Prediction, Military-Industrial Kurier, 2013: 1-12.
2. M. Raska and R. A. Bitzinger, Russia's Concept of Hybrid Wars: Implications for Small States, RSIS Commentary, 2015: 1-3.
3. Qiao Liang and Wang Xiangsui, Unrestricted Warfare, PLA Literature and Arts Publishing House, Beijing, Feb 1999.
4. T. Bunde and A. Oroz, Munich Security Report, Munich Security Conference Foundation, Munich, 2015.
5. A. Pikulicka-Wilczewska and R. Sakwa, Ukraine and Russia: People, Politics, Propaganda and Perspectives, E-International Relations Publishing, Bristol, England, 2015.
6. C. Ionita, Potential National Measures to Counter Hybrid Warfare, Romanian Military Thinking, 2/2015: 17-27.
7. V. Buta, Perspectives of the Evolution and Influence of the Hybrid Warfare Concept, Romanian Military Thinking, 3/2015: 11-32.
8. Raska and Bitzinger, Hybrid Wars, 1-3.
9. Ionita, Hybrid Warfare, 21.
10. F. G. Hoffman, Hybrid Warfare and Challenges, Small Wars Journal, Issue 52, 1st Quarter 2009. http://smallwarsjournal.com/documents/jfqhoffman.pdf
11. The Regional Security Architecture Programme, Institute of Defence and Strategic Studies, The Future of the ADMM/ADMM-Plus and Defence Diplomacy in the Asia Pacific, S. Rajaratnam School of International Studies, Nanyang Technological University, 17 Nov 15.
12. A. E. Varisco, Towards a Multi-Polar International System: Which Prospects for Global Peace?, E-International Relations Students, 3 Jun 2013. http://www.e-ir.info/2013/06/03/towards-a-multi-polar-international-system-which-prospects-for-global-peace/
13. J. Mariani, B. Williams, and B. Loubert, Continuing the March: The Past, Present, and Future of the IoT in the Military, Deloitte University Press, 6 Aug 2015.
14. Official Releases, Singapore Deploys Unmanned Aerial Vehicle Task Group and Institutional Trainers to Afghanistan, Ministry of Defence, Singapore, 27 Aug 2010. http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/ 2010/aug/27aug10_nr.html#.V0lErPl97IU
15. Koh Eng Beng, Protecting Singapore's Skies 24/7, Cyber Pioneer, Ministry of Defence, Singapore, 1 Sep 2014. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2014/sep14_cs.html#.V475vtKGPIV
16. Ong Hong Tat, Five for the Fliers, Cyber Pioneer, Ministry of Defence, Singapore, 2 Sep 2013. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/sep13_cs.html#.V476W9KGPIV
17. Official Releases, Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2016, Ministry of Defence, Singapore, 8 Apr 2016. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/07apr16_speech1.html#.476vdKGPIV

18. Press Release, SLD16 – Minister's Plenary Speech (Regional Security Challenges 15 Years On – Same Plot Different Cast), Ministry of Defence, Singapore, 5 Jun 2016. http://www.gov.sg/resources/sgpc/media_releases/mindef/press_release/P-20160605-1

19. Official Releases, Reply by Minister for Defence, Dr Ng Eng Hen, to Parliamentary Question on Singapore's Deployment of Support to the Anti-ISIS Coalition, Ministry of Defence, Singapore, 28 Jan 2016. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/19jan15_ps.html#.477VNKGPIV

20. Official Releases, Speech by Dr Ng Eng Hen, Minister for Defence, at Committee of Supply Debate 2015, Ministry of Defence, Singapore, 5 Mar 2015. http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05mar15_speech.html#.V477wNKGPIV

SLTC Wong Hin Kai is currently the Head of Concepts and Technology Office in Air Plans Department. An Air Warfare Officer (AWO) (Command, Control and Communications) (C3) by vocation, he attended the Indonesian Command and Staff College in 2009. SLTC Wong holds a Bachelors of Engineering (Hons, 1st Class) from Sydney University and a Masters of Science in Management of Technology from the National University of Singapore (NUS).

MAJ Anthony Lau Kai Heng is an AWO (Ground-Based Air Defence) (GBAD) by vocation and is currently a Branch Head in Air Plans Department. He attended the 45th Goh Keng Swee Command and Staff Course in 2014 and holds a Bachelors in Mechanical Engineering (Hons, 2nd Class Upper) from NUS.

CPT James Yong Dun Jie is an AWO (Command, Control & Communications) (C3) by vocation. He is currently Planning Officer (Air), Joint Operations Planning Branch (JOPB) in Joint Operations Department. CPT Yong graduated from University College London with a Bachelors of Science in Statistics, Economics and Finance with Honours, and a Masters of Science in Operations Research from Columbia University.

Technologies in Hybrid Warfare: Challenges and Opportunities

by ME6 Gabriel Tham, CPT Edward Wong & ME4 Kelvin Kuo Kai Ming

Abstract:

In recent years, hybrid warfare has become increasingly widespread, comprising various conventional and non-conventional means of warfare, as well as non-military options. While technological progress will generate more opportunities, it can also bring about threats to a country. For instance, drone-related technologies pose a sizeable threat due to their accessibility and low cost, enabling mass production and swarm tactics. For Singapore, the Republic of Singapore Air Force (RSAF) will also have to consider methods of minimising collateral damage in air strikes, to alert civilians to impending air strikes, although such technologies are not without limitations. Electromagnetic Pulse (EMP) weapons also pose a significant threat to Singapore, and to combat these, the RSAF can choose to employ active or passive systems. Ultimately, continual technological development is essential for the RSAF to maintain its edge over potential aggressors.

Keywords: Hybrid Warfare, Technology, Drones, Collateral Damage, Weapons of Mass Destruction

INTRODUCTION

Hybrid warfare has attracted the attention of many militaries across the world, especially with the rise of global terrorism and the increasing reluctance of countries to participate in full-scale conflicts. Past conflicts between Israel and Hezbollah to more recent ones such as the annexation of Crimea all saw the use of hybrid warfare. Hybrid warfare comprises a mixture of traditional military maneuvers and confrontations, non-conventional methods such as guerrilla and cyber warfare, and even non-military options such as economic strangulation aimed to weaken an opponent's political and social will. Similar to many other military developments throughout history, technology continues to shape and evolve military strategies and tactics. The face of hybrid warfare will therefore continue to change as technology advances. This essay aims to explore some key trends in hybrid warfare, and look at how technology can provide opportunities as well as pose threats to the RSAF. It will also discuss some of the possible technologies that the RSAF can explore to overcome challenges associated with hybrid warfare.

CHALLENGE #1: RAPID DEVELOPMENT OF COMMERCIAL DRONES – A NEW THREAT FOR AIR FORCES

While countries pursued military technological advancements to gain a capability edge over potential adversaries in the past, rapid development of commercial technologies and the accompanying low-cost options now pose new challenges to the military. Advancements in the fields of robotics, artificial intelligence, additive manufacturing and nano-materials have not only shortened the product development cycle but have also given rise to a whole range of low-cost, yet effective military options.[1] The availability of low-cost commercial technologies provides an affordable means for militaries to rapidly assimilate these new technologies and evolve their fighting concepts and tactics. On top of that, the use of these low-cost technologies can enable the underdog to overturn capability asymmetry, sometimes forcing their enemies to follow in terms of adapting low-cost technologies in their fighting systems.[2] It is however challenging to do this while having to keep the capability edge in conventional war. Hence, to adapt some of their conventional capabilities, countries would end up investing heavily in adapting or developing their weapons systems to overcome the new threats.

While countries pursued military technological advancements to gain a capability edge over potential adversaries in the past, rapid development of commercial technologies and the accompanying low-cost options now pose new challenges to the military.

There has been an enormous growth in the field of commercial unmanned systems over the past decade. Fully autonomous, cheap and long-range drones have emerged in the mass market for recreational applications. Some recent technological developments in commercial drones have raised several concerns amongst militaries across the globe. First, since they are designed for the mass market, these unmanned systems are relatively low in cost, easily available and easy to use. With their composite construction and very low energy usage, they will be very difficult to detect. Of even greater concern, these small, inexpensive drones are designed to be operated by people with little or no specialised skills and in-house maintenance capabilities. Once equipped with a small explosive payload, it could prove difficult to detect and defend against such weapons of terror. Second, they are becoming increasingly smart. The autonomy of commercial drones is improving as they are equipped with smart technologies such as sensors, advanced navigation systems with GPS, powerful microprocessors, digitally encrypted controls and communications.[3] Non-state actors can now easily produce cheap, smart and deadly drones that could operate co-operatively in swarm tactics to saturate and overwhelm a military air defence.

Last but not least, these drones are becoming cheaper. With additive manufacturing, the cost of manufacturing customised high-end drones will go down. Recently, researchers in England have prototyped a printed drone that will cost roughly $9 a copy. This drastically opens the access of inexpensive high end drones to both state and non-state actors. For example, the Chinese have fielded the Harpy Unmanned Combat Air Vehicle (UCAV). Initially developed in the 1990s by Israel as an anti-radar system, the Chinese version has a range of 500 km and a 32kg warhead with multiple types of seeker heads. One Chinese configuration has 18 Harpies in box launchers mounted on a single truck bed (other configurations use 6 launchers per truck).[4] Essentially, these are expendable drones capable of saturating defensive systems. This system represents a first step towards inexpensive swarms.

There are many ways that these commercial drones could be used and become a threat to the Air Force. The most obvious is to use these drones as a weapon. Without the need for sophisticated navigation systems or target recognition, these autonomous drones can easily fly a pre-programmed route to a target area and inflict damage on any of the designated targets.

Example of a Commercial Unmanned Aerial Vehicle that could be used as an airborne obstacle

Navigation could be done through GPS or Google Maps, and cheap and commercially available optical recognition hardware and software would provide rough targeting. Commercially available quadcopters, which are able to carry loads such as a GoPro camera weighing 100g and with endurance of over 30 minutes, could easily be modified for military use. In the past, skilled machinists with high-quality machine tools were required to equip commercial drones with explosively formed penetrators (EFPs). However, in the last few years, additive manufacturing has advanced to the point where such EFPs could be 'printed'.

For Air Forces, this approach poses a major threat to the air power generation. Instead of engaging in an air campaign, the adversary could send hundreds or even thousands of small drones after each aircraft at its home base. Larger-sized support aircraft, such as tankers, airborne early warning and control aircraft (AWACs), and transports, are even more vulnerable to this form of attack. If drones were equipped with larger explosives, aircraft protected by shelters, radars, fuel systems and ammunition dumps could be vulnerable too. The massive deployment of these drones could even hinder the launch capabilities of the Air Force. Acting as airborne obstacles, these drones could effectively create a blockage over any airfield.

Anti-Drone Technologies

To overcome the threats posed by commercial drones, Air Forces will need to invest in anti-drone technologies. Many technologies have emerged to overcome the challenges posed by commercial drones. In order to effectively deal with this new threat, technologies to detect and then terminate these drones are required. Detecting these commercial drones is quite difficult, especially in a busy urban environment. These small and slow-moving drones render traditional radar and imaging technologies ineffective.[5] To overcome this, some anti-drone systems use composite radar and imaging techniques to detect incoming drones. The Sky Archer Counter Micro-UAV System, primarily uses a visual detection system but can be upgraded with radar to enhance detection. A system is being developed by Singapore Technologies Electronics which would allow users to watch over specific areas where UAVs are not permitted.[6] Newer technologies that leverage on acoustics are also being explored. The DroneShield system is one such solution that centres on detecting, identifying and locating an incoming drone based on the sound it makes. The system will run every sound it hears through a library which contains the noises made by different types of drones. If a match is found, it can alert a human operator to confirm and track the incoming drone.

After detection, the termination or disabling of these drones could be done in a few ways. The most popular approach currently is to disable the drone through radio frequency jamming. The most rudimentary method is to flood the radio frequency band that the drone is operating in. This will disrupt the connection between the controller and the drone, making the drone uncontrollable and ultimately causing it to crash. However, modern commercial drones employ spread spectrum communications, making it difficult to jam the control frequencies. Other more elegant methods such as GPS spoofing or hacking into the drone's control systems are being developed. Another approach to disable a drone requires a physical net to be deployed onto the drone. Systems such as Skywall by OpenWorks Engineering and MP200 by MALOU Technologies use propelled or drone-carried nets to take down any hostile drones. However, this approach requires training and specialised skills and may not be effective when dealing with a saturation attack by a swarm of autonomous drones.

Directed-Energy Weapon (DEW) – A Means to Overcome Drone Saturation

To overcome a swarm of autonomous drones, the traditional means of jamming each drone or shooting them down with a physical net is no longer effective. The rise of low cost drones has enabled the mass deployment of autonomous drones, particularly by state actors aiming to use unconventional means to wage hybrid warfare. Directed-Energy Weapons (DEW) provide a low cost means to overcome such attacks. One such system is Lockheed Martin's newly developed Athena (Advanced Test High Energy Asset) weapon, which uses a 30-kilowatt fibre laser.[7] It was tested against a small Phantom quadcopter drone's engine and camera with precision at over a kilometre away. The system is capable of creating a hole through five-centimetre thick steel, such as that of the engine of a truck, in seconds. Most importantly, each shot cost less than a dollar. The cost-efficiency of such counter-measures is critical when dealing with application of drone swarm. DEWs have applications that extend beyond commercial drones; they also provide a cost-effective defence against rockets and can replace expensive missiles. Compared to the Iron Dome used by the Israel Defense Forces (IDF) which costs around $20k per interception, DEW provides a much cheaper alternative to combat short-range rockets fired by Hamas and Hezbollah. Past lasers were inefficient because of their large size, large power demand and inability to cool. However, with advancements in laser technology, these shortcomings were mitigated and lasers became viable weapons in the directed energy arsenal. For example, Boeing has developed the (BA) YAL-1 Airborne Laser, a megawatt chemical laser system built in 2002 that can be mounted inside a modified Boeing 747. With the advancement in DEW technologies, we can expect to see more of such systems deployed in airborne platforms.

CHALLENGE #2: INCREASED DIFFICULTY FOR AIR STRIKE OPERATIONS IN DENSELY POPULATED ENVIRONMENT

When the adversary is inferior, either in terms of military capability, size or technology, it may choose to employ non-conventional means to overcome this asymmetry. The adversary will leverage on any advantage it can attain to mitigate the advantage its enemy has in conventional warfare. In some instances, it could hide among civilian infrastructure that should not be targeted by conventional military actions, such as schools, hospitals or religious buildings, and adopt such civilian infrastructure as its headquarters or staging areas for military operations. This makes it difficult for conventional militaries to execute their mission while trying to comply with international agreements such as the Geneva Conventions. The Geneva Convention states that:

> *"The presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations. The parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations."*[8]

These scenarios present a 'Catch-22' for militaries between neutralising the threat with possible civilian casualties and inaction that could lead to more friendly casualties. The Gaza–Israel conflict is one such example. Hamas fighters understand the restrictions most conventional militaries have. Knowing that places of worship, residences and hospitals can easily be reckoned as illegitimate military targets in the eyes of the world, they purposely used these places as weapon caches, shelters for military personnel, concealed tunnels and command posts. The IDF was then forced to make difficult decisions of whether to conduct air strikes on these civilian buildings, many of which were even schools, hospitals and mosques within Gaza.[9] In fact, there were instances of IDF intelligence clearing a target for an air strike, only to find that the battle damage assessment showed no signs of Hamas militants.[10] It is very likely that the militants escaped through their network of tunnels. Not only did Hamas take advantage of the protection that these places provided, they also exploited the resultant collateral damages from the IDF air strikes and raised dissent in the war-torn people against the IDF.[11]

When the adversary is inferior, either in terms of military capability, size or technology, it may choose to employ non-conventional means to overcome this asymmetry.

In densely-populated Gaza, where there are almost two million people within an area of 380 square kilometres, the fear of inflicting collateral damage remains despite advancements in precision munitions. Regardless of the enhanced precision, any effective munitions required to destroy the enemy's weapons cache or command posts would still have a certain blast radius, thus still affecting population around the target. With the enemy hiding in the midst of civilians, launching rockets into Israel and quickly finding cover back among the masses of densely populated residential area, the IDF found it challenging to be effective in the execution of their air strikes.

Wreckage resulting from an air strike in densely-populated Gaza

'Knock On Roof' – Integration of Commercial-Military Technologies

In order to minimise civilian casualties in the conduct of precision air strikes, the IDF adopted a 'Knock on Roof' concept. Phone calls or Short Message Service (SMS) was first sent to potential targets.[12] Subsequently, a dummy missile with little to no explosive load would be dropped at the targeted building, the actual 'Roof Knock', informing building inhabitants of the imminent air strike.[13] Finally, an actual bomb would strike the target, taking out the enemy's weapons cache or command posts. The IDF hoped that this approach would provide Gaza civilians with an adequate warning to react to the incoming air strike. The IDF also claimed that it conducted persistent Intelligence, Surveillance and Reconnaissance on these targeted buildings to understand how many people were in the buildings at any one time, allowing them to conduct accurate assessments of the number of residents present.

It is not clear how the IDF delivered the warning calls and SMS to unknown phone numbers, but the attributes are similar to commercial Cellular Broadcast technologies. For example, Alcatel-Lucent developed the Broadcast Message Centre (BMC) to send text alerts to mobile users based on their geographic location. The BMC was initially developed to broadcast warnings to locations, which could be experiencing a gas leak, chemical spillage or natural disaster, thereby providing early notice for evacuation. BMC works through cellular network and infrastructure where the requestor first sends a required message to an alert gateway. This is relayed to the BMC, which delivers the messages to the respective carriers to broadcast the message to phones within the allocated area.[14]

Long Range Acoustic Device – An Alternative to 'Roof Knock'

However, the 'Knock on Roof' concept has its limitations. The warnings before an actual air strike may not be effective. The 'Roof Knock' is essentially still a munition—albeit without the explosives—and is still capable of causing damage on unstable roof structures. In some cases, the 'Roof Knock' caused damage to the building or people inside before the actual strike occurred.[15] In addition, it is still subject to the same errors of a live strike. A typical bomb guidance unit has a Circular Error Probability (CEP) of 5 to 30m. This CEP in the context of a dense, urban environment could translate to potential misses of the intended target. Also, 'Roof Knock' could easily be mistaken for another nearby explosion, causing residents to disregard these warning shots. Even phone calls or SMS could be easily missed, rendering it difficult to ensure effective warning.

While phone calls or 'Roof Knock' may not provide enough coaxing for residents to evacuate a building that has become an imminent target, Long Range Acoustic Device (LRAD) could potentially be a viable alternative in the future. LRAD is able to create a directed blast of high volume sound waves, which are irritating, loud and potentially painful, over long distances. The military-grade LRAD 2000X can transmit voice commands up to 162 decibels (dB) with a range up to nine kms away.[16] LRAD would be able to provide a more effective Roof Knock as there would be no ambiguity of where the noise is coming from and this could reduce errors inherent to dropping aerial munitions. If directed voice commands are not 'persuasive' enough, LRAD could apply increased power to 'encourage' residents to vacate a building. Human discomfort begins when sounds increase past 120dB. LRADs have recently been used in the Ferguson riots in Missouri, USA as a method of crowd control.[17]

Wikipedia

Long Range Acoustic Device capable of producing directed blasts of high volume sound waves.

CHALLENGE #3: EMERGENCE OF CHEAP AND ACCESSIBLE WEAPONS OF MASS DESTRUCTION

Traditional Weapons of Mass Destructions (WMD), including biological, nuclear or chemical weapons have become less acceptable to be used in view of the inhumane effects they bring on both their human targets and the environment. These weapons not only have the ability to wipe out whole cities or states but also have the prolonged ill-effect of rendering the area unusable by enemy forces. Therefore, in the past, WMDs were employed mainly by terrorist organisations that aimed to strike fear in a population or by state actors who utilised them as a last resort. However, modern technologies have brought about a new range of WMDs. Besides cyber warfare that could wreak disasters on national infrastructure such as power, water or transportation, another such means is Electromagnetic Pulse (EMP) weapons.

EMP weapons will provide potential adversaries with an avenue of initial attack, without the remaining ill-effects of a nuclear strike

Electromagnetic Pulse Weapons

Nuclear weapons have been around since World War II (WWII), and the most well-known employment was by the United States (US) on Nagasaki and Hiroshima leading up to the eventual Japanese surrender. 'Fat Man' and 'Little Boy' were aerially dropped. Employment of these weapons has become more diverse since then. Though the majority of a nuclear weapon's destruction is caused by very high temperatures and pressures coupled with an expanding shockwave, there is also damage caused by an accompanying EMP. For example, during nuclear weapons testing in 1962, codenamed Starfish Prime, a 1.4 megaton warhead which detonated 386 km above the earth was launched from Johnson Island in Ohio, USA. The EMP from this weapon was strong enough to affect the electrical grid in Hawaii 1148km away, resulting in blown streetlights, telephone outages and radio blackouts.[18]

EMP weapons will provide potential adversaries with an avenue of initial attack, without the remaining ill-effects of a nuclear strike. Compared to the requisite knowledge to develop a full atomic weapon, developing an EMP weapon requires relatively less know-how. With the ability to cripple city networks without the adverse effects of nuclear fall-out and destruction, EMP weapons would be attractive to state and non-state actors in hybrid warfare. Many countries have started developments of a kamikaze drone. These will be employed during time critical missions where the operator will acquire the target before the drone strikes and explodes itself. Kamikaze drones such as the Harop by Israel Aerospace Industries and AeroVironment's Switchblade can be armed with an EMP payload to deliver the first blow to an adversary.[19] As demonstrated by nuclear tests, even small yield nuclear weapons may have big EMP ramifications. Radars, aircraft and air defence systems could easily be disabled within the first blow and would no longer be useful for the rest of the air campaign.

EMP weapons also provide militaries with more surgical strike options. Since EMP weapons are only effective against electronics, they provide a means to knock out an opponent's command posts and weapons systems without the fear of causing civilian casualties. The United States Air Force has recently modified cruise missiles to carry a high-powered energy weapon. This missile can be set with a pre-determined flight path and is able to send up to 100 microwave pulses, which could short electronics on the ground.[20] The use of EMP weapons does face some challenges. Operating in environments where friendly ground troops are in forward-deployed positions would enforce limitations. Frying friendly communications, and weaponry in some cases, could prove fatal to troops on the ground.

Closer to home, EMP weapons can threaten our very way of life. Should an EMP be detonated nearby, it would leave Singapore without electricity, communications, transportation, fuel, food or even running water. The fact that Singapore is a small island state makes it geographically even more susceptible to EMP weapons as they could affect the country's entire electrical grid, taking months or even years to rectify.[21] The RSAF can also be vulnerable to an EMP attack as aircraft, Ground-based Air Defence systems, radars and UAVs all make up the RSAF's order of battle, none of which are absolved of the EMP threat in view of their reliance on electronic systems. The RSAF must be conscious of the threat and employ the necessary defensive measures to ensure the safety of Singapore's skies.

PASSIVE AND ACTIVE DEFENCE AGAINST EMP WEAPONS

Passive defences could be employed to guard electronic systems from the EMP pulses produced by low-yield Hydrogen bombs. The concept of a Faraday cage is by no means new technology (as it was invented by Michael Faraday in 1836) and can be applied to defend against EMP attacks.[22] Ground-based critical systems such as radars, servers and operations nodes as well as aircraft hangars are typically hardened against kinetic munitions and the hardened facilities can be easily improved with a simple Faraday cage to provide a passive, last-layer defence against EMP weapons.

Wikipedia

Second successful launch of the Arrow-3 interceptor in January 2014.

However, it is not enough to rely solely on passive systems. The deadliness of high-altitude nuclear attacks is largely proportional to the altitude at which they are detonated. As such, an early-warning, missile-interception system that could prevent such a missile from reaching critical altitude could be adapted to target EMP missiles. Long range systems such as the Israeli Arrow would be able to undertake high altitude interceptions at long ranges, effectively covering a wide swath of airspace. The Arrow-3 has a range of 90km and maximum altitude of 50km. This is significant upgrade to Israel's Patriot PAC-2 local missile defence system which has a range of 40km.[23]

CONCLUSION

Whether by addressing threats such as commercially-available drones or operating in densely-populated environments, hybrid warfare poses several new challenges to the RSAF. The rise of commercial drones, being cheaper and smarter, provides opportunities for the RSAF to employ swarm techniques. However, the fact that such technology is equally-accessible to non-state actors or adversaries of lower technological capability poses new challenges to the RSAF. These drones can now be used as cheap weapons or even co-operatively operated to hinder launch and recovery operations. As the defence and security industries develop new technologies in the detection and termination of these drones, the RSAF will need to explore low cost options such as DEW to overcome potential saturation attacks by a swarm of low-cost drones.

Even with increased precision, air strikes will increasingly become more difficult as we fight in a more densely-populated environment. The enemy is expected to take cover in populous areas, making it difficult to conduct air strikes without collateral damage and civilian casualties. While the IDF developed a 'Knock on Roof' concept, it had limited success. New technologies that leverage commercial communications as well as specialised systems such as LRAD can be used to overcome some of the challenges.

Finally, the RSAF will need to closely monitor the development of EMP weapons, which can be very effective against the electronics and networked systems in any Air Force. While EMP weapons can provide new surgical strike options for the RSAF, there are also challenges to their viable application. Friendly forces in the field and civilian infrastructure at home are also susceptible to its adverse effects, which posing limitations to their application in both offensive and defensive settings.

Improvements in technology have heralded trends in hybrid warfare that amplify threats to the RSAF. They would require the RSAF to seek out possible solutions to combat these threats. While the threats listed above are urgent and critical, they are definitely not exhaustive. Combating nuclear, space and cyber threats continue to be at the forefront of Air Forces' priorities in the foreseeable future. Weapons which are cost-effective in dealing with the identified threats become all the more important in a prolonged period of conflict. The RSAF will have to continually update its weapons systems and concept of operations by sieving out the trends ushered in by new technology, so as to maintain its technological edge over any possible adversaries.

ENDNOTES

1. Rusling, Matthew. "For the Military, a Future of Hybrid Wars." National Defense Magazine. September 1, 2008. Accessed July 7, 2016. http://www.nationaldefensemagazine.org/archive/2008/September/Pages/Hybrid_Wars.apsx
2. Hoffman, Frank G. "Hybrid Warfare and Challenges." Joint Force Quarterly. February 2, 2009. Accessed July 15, 2016. http://smallwarsjournal.com/documents/jfqhoffman.pdf
3. Johnson, David. "Military Capabilities for Hybrid War." RAND Corporation occasional paper series. June 26, 2010. Accessed July 15, 2016. http://www.rand.org/content/am/rand/pubs/occasional_papers/2010/RAND_OP285.pdf
4. Hambling, David. "Drone swarms will change the face of modern warfare." Wired. Accessed July 6, 2016. http://www.wired.co.uk/article/drone-warms-change-warfare

5. Teo, Benita. “Transforming the SAF to meet new challenges.” Cyberpioneer. June 30, 2015. Accessed July 13, 2016. https://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2015/jun/30jun15_news3.print.img.html

6. “ST Electronics Showcases Smart Solutions at Singapore Airshow 2016.” Electronics Review. Accessed July 15, 2016. http://www.stee.stengg.com/pdf/publication/Vol29No1/Event 3.pdf

7. “High-energy laser weapons target UAVs.” C4ISRNET. Accessed July 13, 2016. http://www.c4isrnet.com/story/military-tech/uas/2016/02/19/high-energy-laser-weapons-target0uavs/80553744

8. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule97

9. Sherwood, Harriet. "In Gaza, Hamas Fighters Are among Civilians. There Is Nowhere Else for Them to Go." The Guardian. July 24, 2014. Accessed July 14, 2016. https://www.theguardian.com/world/2014/jul/24/gaza-hamas-fighters-military-bases-guerrilla-war-civilians-israel-idf

   "UN Report Confirms Hamas Stored and Fired Weapons from UN Schools." The Tower. April 28, 2015. Accessed July 14, 2016. http://www.thetower.org/1955-un-report-confirms-hamas-stored-and-fired-weapons-from-un-schools/

10. Soffer, Ari. "French TV Shows More Evidence of Hamas Hiding Behind Civilians." - Defense/Security. August 5, 2014. Accessed July 14, 2016. http://www.israelnationalnews.com/News/News.aspx/183759#.V3yyUuZ97Vo.

11. Hirschauge, Orr. "Israel and Hamas Take Fight to Social Media." WSJ. July 23, 2014. Accessed July 14, 2016. http://www.wsj.com/articles/israel-and-hamas-take-fight-to-social-media-1406130179

12. Erlanger, Steven, and Fares Akram. "Israel Warns Gaza Targets by Phone and Leaflet." The New York Times. July 08, 2014. Accessed July 14, 2016. http://www.nytimes.com/2014/07/09/world/middleeast/by-phone-and-leaflet-israeli-attackers-warn-gazans.html?_r=1

13. Gayle, Damien. "How Israel Tells Gaza's Residents to Get out of Buildings before They Are Blown Apart: Footage Emerges of Controversial 'knock on the Roof' Air Strike Warning." Mail Online. July 14, 2014. Accessed July 14, 2016. http://www.dailymail.co.uk/news/article-2691302/Watch-Israels-controversial-knock-roof-air-strike-warning-condemned-human-rights-groups.html

14. Team, Gizmag. "Mobile Broadcast Message Center Can Text All Cell Users in a given Geo-location." Mobile Broadcast Message Center Can Text All Cell Users in a given Geo-location. November 17, 2010. Accessed July 14, 2016. http://www.gizmag.com/mobile-broadcast-message-center-text-all-cell-users-given-geo-location/16965/

15. Lister, Tim, and Salma Abdelaziz. "Israeli Military's 'knock on Roof' Warnings Criticized by Rights Groups." CNN. July 15, 2014. Accessed July 14, 2016. http://edition.cnn.com/2014/07/15/world/meast/mideast-israel-strike-warnings/

16. Wilson, Tracy V. "How LRAD Works." HowStuffWorks. March 3, 2006. Accessed July 14, 2016. http://science.howstuffworks.com/lrad.htm

17. "What Are 'sound Cannons' and Why Are Police Using Them in Ferguson?" The Week UK. November 14, 2014. Accessed July 14, 2016. http://www.theweek.co.uk/us/61501/what-are-sound-cannons-and-why-are-police-using-them-in-ferguson

18. Kelly-Detwiler, Peter. "Failure to Protect U.S. Against Electromagnetic Pulse Threat Could Make 9/11 Look Trivial Someday." Forbes. July 31, 2014. Accessed July 14, 2016. http://www.forbes.com/sites/peterdetwiler/2014/07/31/protecting-the-u-s-against-the-electromagnetic-pulse-threat-a-continued-failure-of-leadership-could-make-911-look-trivial-someday/#2bfc4a367fcdd

    "Nuclear Weapon EMP Effects." Nuclear Weapon EMP Effects. Accessed July 20, 2016. http://fas.org/nuke/intro/nuke/emp.htm

19. Fishler, Eliana. "NEWS SUCCESSFUL FLIGHT DEMONSTRATIONS FOR HAROP LOITERING MUNITIONS." June 7, 2015. Accessed July 14, 2016. http://www.iai.co.il/2013/32981-46464-en/MediaRoom_News.aspx

    "Switchblade Tactical Missile System." Army Technology. Accessed July 14, 2016. http://www.army-technology.com/projects/switchblade-tactical-missile-system/

20. Chang, Lulu. "U.S. Air Force Confirms Boeing's Electromagnetic Pulse Weapon." Digital Trends. May 26, 2015. Accessed July 14, 2016. http://www.digitaltrends.com/cool-tech/us-air-force-confirms-boeings-electromagnetic-pulse-weapon/

21. B, G. "Six Common Misconceptions About EMP - ProtecTgrid." ProtecTgrid. Accessed July 20, 2016. http://www.protectgrid.com/civil-defense-2-0/six-common-misconceptions-about-emp/

    Huessy, Peter. "Electronic Doomsday for the US?" Gatestone Institute. January 13, 2016. Accessed July 20, 2016. http://www.gatestoneinstitute.org/7214/electro-magnetic-pulse-emp

22. Emanuelson, Jerry. "Electromagnetic Pulse Protection - EMP - Futurescience.com." Electromagnetic Pulse Protection - EMP - Futurescience.com. Accessed July 20, 2016. http://www.futurescience.com/emp/emp-protection.html

    Chandler, Nathan. "How Faraday Cages Work." HowStuffWorks. Accessed July 20, 2016. http://science.howstuffworks.com/faraday-cage1.htm

23. Defense Industry Daily Staff. "Israels Arrow Theater Missile Defense." Defense Industry Daily RSS News. June 16, 2015. Accessed July 20, 2016. http://www.defenseindustrydaily.com/israel-successfully-tests-arrow-theater-missile-defense-01571/

ME6 Gabriel Tham is currently the Commanding Officer of 808 SQN. Prior to this, he was the Head Joint Logistics Plans and Resource Branch in Joint Logistics Department (JLD) and Senior Force Transformation Officer (Logistics) in Joint Plans & Transformation Department (JPTD). He also held command appointments in UAV Command and Air Defence & Operations Command (ADOC), and staff appointment in Air Engineering & Logistics Department (AELD) and Defence Science & Technology Agency (DSTA). He attended the Peoples' Liberation Army Air Force Command and Staff Course in 2015. He currently holds a Master in Science in Electrical Engineering (Distinction) from Naval Postgraduate School, a Masters of Science in Defence Technology and Systems from NUS and a Masters in Military Studies from China. He graduated from NUS with a Bachelors of Engineering (Electrical Engineering) and a Minor in Management in Information Systems in 2003.

CPT Edward Wong is a UAV Pilot by vocation and is currently a Staff Officer in Air Operations Department. CPT Wong was previously a pilot in 119 SQN.

ME4 Kelvin Kuo Kai Ming is an Air Force Engineer by vocation and is currently a Staff Officer at Joint Communications & Information Systems Department (JCISD). ME4 Kelvin graduated from Imperial College London with a Masters in Engineering (Aeronautical Engineering).

Cyber Threats in Hybrid Warfare: Securing the Cyber Space for the RSAF

by LTC Anthony Wong, MAJ Christopher Eng, CPT Ronald Loh Ming Yao & CPT Jeffrey Ng

Abstract:

According to the authors, as cyber attacks are gaining traction, it is essential for the Republic of Singapore Air Force (RSAF) to develop a comprehensive cyber defence strategy to ensure that our military networks are not compromised. This essay focuses on how cyber attacks have evolved over the years and how other established militaries addressed the cyber threat challenge. Drawing insights from these observations and in the face of an increasingly sophisticated cyber threat environment, the authors highlight that the RSAF would need to develop a multi-layered cyber defence strategy to guard its capabilities and operational effectiveness in peace and war.

Keywords: Warfare, Cyber Space, Cyber Attack, Evolution, Technology

INTRODUCTION

> *"Cyber attacks are integral parts of hybrid warfare... Adversaries can cripple key operating systems of target countries, steal their state and people's secrets, [and] invade the hearts and minds of people, all without stepping foot onto their soil."*
>
> *-Dr Ng Eng Hen, Minister for Defence*[1]

In the past decade, the world has progressed towards a new paradigm where cyber warfare can fundamentally alter the way future wars are fought. Cyber attacks were also waged as part of hybrid warfare in which adversaries (nation-state, state-funded or non-state actors) exploited the cyber domain to target capabilities and institutions that relied heavily on networks.[2] In addition, the evolving cyber conflicts occur not only in wartime—cyber attacks have been occurring on a persistent basis even in peacetime or during periods of low intensity conflicts.

While cyber attacks such as cyber crime and cyber espionage have dominated global news headlines, it is the growing spectrum of state-sponsored cyber attacks driven by strategic or military objectives that have become a major cause of concern for national security. Military establishments in many countries recognise the ramifications of cyber warfare. The United States (US) has declared cyber space as the fifth domain of warfare—in addition to the air, land, sea and space domains—and they have invested considerable resources in developing cyber strategies to deal with this emerging security threat.

With the increased use of cyber attacks gaining traction, it is essential for the RSAF to develop a comprehensive cyber defence strategy to ensure that our military networks are not compromised. This essay focuses on how cyber attacks have evolved over the years and how other established militaries addressed the cyber threat challenge. Drawing insights from these observations and in the face of an increasingly sophisticated cyber threat environment, the RSAF would need to develop a multi-layered cyber defence strategy to guard its capabilities and operational effectiveness in peace and war.

EVOLUTION OF THE CYBER THREAT SPECTRUM

Cyber threats have existed in various forms since the proliferation of the internet. As shown in *Figure 1*, the cyber threat spectrum could range from malicious pranks by individual hackers, profiteering through criminal activities, conduct of espionage, to nation-state cyber warfare.

In the 1990s to early 2000s, cyber attacks were traditionally conducted by hackers as a form of malicious prank or criminal groups committing cyber crime. Notable cyber threats during these early years included *SoBig*, *Bagle* and *My Doom* that affected millions of computers world-wide. These viruses or worms made malicious changes to the infected computers and generated millions of spam-messages. The more advanced viruses such as *My Doom* had the capability to control millions of computers to conduct Distributed Denial-of Service (DDoS) attacks.[4]

The potential of viruses and worms to control computers gave rise to botnets, which were used by criminal groups to commit cyber-crimes. These groups, using virus-controlled botnets, conducted DDoS attacks to extort money from businesses.[5] Botnets were also used to conduct phishing attacks with the purpose of stealing someone's identity for profiteering. According to *The Economist*, cyber-crime organisations such as the Russian Business Network sold their services to any bidders, from cyber criminals and hacktivists to organisations that wanted to steal secret data.[6]

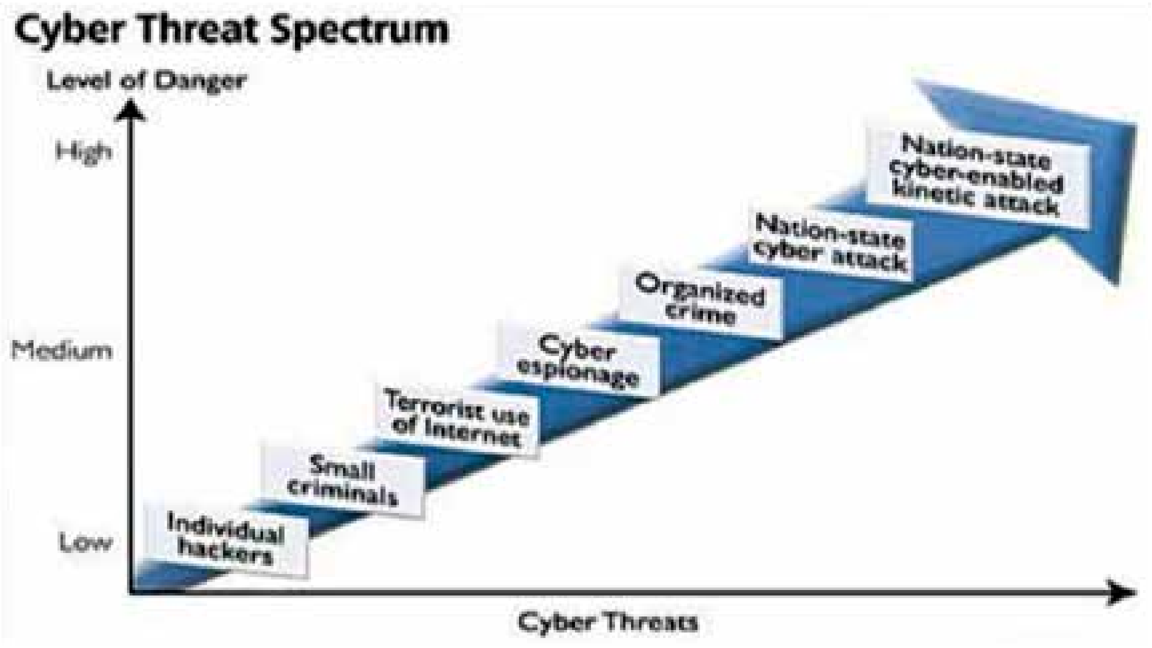


Figure 1: Spectrum of Cyber Threats.[3]

THE RISE OF STATE-LED CYBER WARFARE

Nation-state cyber attacks soon came into prominence with Russia being suspected of leveraging cyber operations to achieve its military and strategic objectives in two separate campaigns. The first incident occurred in 2007 when the Estonian government decided to remove the Bronze Soldier, a memorial commemorating the Soviet liberation of Estonia from the Nazis. Pro-Russian hacktivists, presumably under the sponsorship of the Kremlin, struck several key Estonian institutions through DDoS cyber attacks, which brought a high-tech economy and government to their knees.[7] The second operation was during the Russian-Georgian war of 2008, where cyber attacks shut down the Georgian government and local news website just before the Russian military invaded the town of Tskhinvali in Georgia, giving the Russian military total dominance over Georgia's information space.[8]

Besides Russia, Israel has also demonstrated the ability to integrate non-kinetic cyber attacks with kinetic attacks during military operations in 2007. Under Operation Orchard, the Israeli Defense Force (IDF) conducted cyber attacks on Syria's air defence systems, which allowed the Israeli Air Force to enter Syrian airspace undetected to conduct an air strike on the Syrian nuclear facility in the Deir ez-Zor region.[9]

The use of cyber attacks as a force multiplier in military operations—in the case of the Russian-Georgian war and Operation Orchard—generated intense debates amongst military strategists on cyber warfare. Advocates of cyber warfare included Lieutenant General Alexander Burutin, the Russian Deputy Chief of Staff, who predicted that future wars could be won without the physical destruction of enemy troops, "but rather by the suppression of his state and military control systems, navigation and communication systems, and also by influencing other crucial information facilities that the stability of controlling the state's economy and Armed Forces depends on."[10] Other prominent figures, such as former United States (US) Secretary of Defence Leon Panetta, also acknowledged that cyber warfare represents the battleground for the future and the potential for the next Pearl Harbour could very well be a cyber attack.[11]

The ability for nation-states to launch cyber attacks to disrupt or damage critical infrastructure through non-kinetic means was also effectively demonstrated through *Stuxnet*, which was commonly known to be developed by the United States (US) and Israel to target the Natanz nuclear enrichment plant in Iran. *Stuxnet* was designed to subvert the control systems of Natanz's Uranium centrifuges to abruptly speed up or slow down the rotor speed to the point of self-destruction while simultaneously disabling the plant's alarm systems.[12] The infiltration of *Stuxnet* into Natanz's control system demonstrated that cyber attacks could be conducted even if the targeted systems were 'off-the-grid'.

As the world came to terms with *Stuxnet*, Israel was suspected to have developed *Flame*, a highly sophisticated espionage programme that infected mainly Middle-Eastern countries, especially Iran.[13] In 2011, a worm similar to *Stuxnet*, codenamed *Duqu*, was also discovered. *Duqu's* purpose was to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, and thereby enable its designer to conduct a future attack more easily against another third party.[14]

STUXNET AND BEYOND: THE RISE OF ADVANCED PERSISTENT THREATS

The development of highly sophisticated malware such as *Stuxnet*, *Flame* and *Duqu* represented a key shift from traditional DDoS and mass phishing cyber attacks towards Advanced Persistent Threats (APTs) in cyber warfare. According to the National Institute of Standards and Technology, APT is "an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors."[15] APT attacks are typically highly targeted with a clear objective, which could range from cyber-espionage to cyber attacks on critical infrastructures, operating systems or organisations. Given the sophistication of APT attacks and the resources required to carry out these attacks, actors behind APT are usually state-sponsored and may operate in tandem with military or state intelligence.[16]

Evidence suggests that current cyber security mechanisms are often ineffective in dealing with APT, which often uses sophisticated means to evade cyber detection. Research showed that the average number of days from infection to identification of the APT was 416 days.[17] For example, a long-running APT codenamed Operation Dust Storm has been active since 2010, but the existence and extent of damage of this APT was only recently revealed. According to security firm Cylance, the hackers behind this operation targeted various organisations in Asia, the US and Europe from 2010 to 2015. These hackers used various means to conduct their cyber attacks, ranging from launching watering holes and phishing attacks to remote access Trojans and zero-day exploits. In 2015, these hackers also leveraged Android backdoors (instead of Windows backdoors) to deliver a strain of malware dubbed 'Misdat', which would allow hackers to gain unauthorised access and control of the infected computer systems. Given that the group was well-organised and well-funded, Cylance researchers believed that this operation involved a nation-state actor.[18]

CHALLENGES IN CYBER DEFENCE

The evolving nature of these highly sophisticated cyber threats highlights three key challenges in cyber defence. First, while passive cyber defences measures can prevent low-level attacks, it is no longer effective in countering sophisticated cyber attacks. APTs are designed to target system vulnerabilities or behaviour analysed through intelligence gathering. They are built to circumvent existing network defences, evade detection, and wait to be triggered before delivering their malicious code to infect the targeted system.

Second, it is easier for a cyber attacker to carry out an attack than it is to defend against it. It is difficult for cyber defence methods to completely eliminate any intrusions as new vulnerabilities in operating software, hardware, and network architecture are constantly being identified. In addition, organisations may not have any indications that their systems have been compromised until the installed malware is triggered to carry out the attack. Therefore, part of an effective cyber defence strategy is to determine a baseline capability to ensure operational continuity. It is also important to strengthen the resilience of networked systems and prevent a steep capability drop after suffering a cyber attack. Thereafter, action plans must kick in to recover to full capability.

Third, the human factor is usually the weakest link in any cyber defence. Any personnel could be targeted for spear phishing and these personnel could inadvertently transfer malware into their own system. Furthermore, an insider who fails to adhere to the established cyber security practices risks introducing malware into even a closed system. The most prominent example would be the *Stuxnet* infection, which was introduced into Natanz's closed network through a USB thumb drive by an employee working in engineering.

CYBER DEFENCE STRATEGY IN THE EVOLVING CYBER THREAT ENVIRONMENT

Given the rise in advanced cyber attacks and the risks it poses to a state's national security, militaries around the world have evolved their cyber defence strategy to address the increasing threats.

US Cyber Strategy

For the US Department of Defence (DoD), the compromise of its classified military networks in 2008 was a wake-up call for the Pentagon to develop a comprehensive cyber defence strategy to counter cyber attacks. The 2008 intrusion was not the only successful cyber attack. According to William Lynn, the then-US Deputy Secretary of Defence, adversaries of the US have also "acquired thousands of files from US networks and from networks of US allies and industry partners, including weapons blueprints, operational plans and surveillance data."[19]

Recognising that passive cyber defence approaches such as firewalls, patching of security vulnerabilities and virus and threat detections are no longer adequate to counter APT, the US developed the concept of active cyber defence in 2010 to complement its passive cyber defence approach. The US DoD

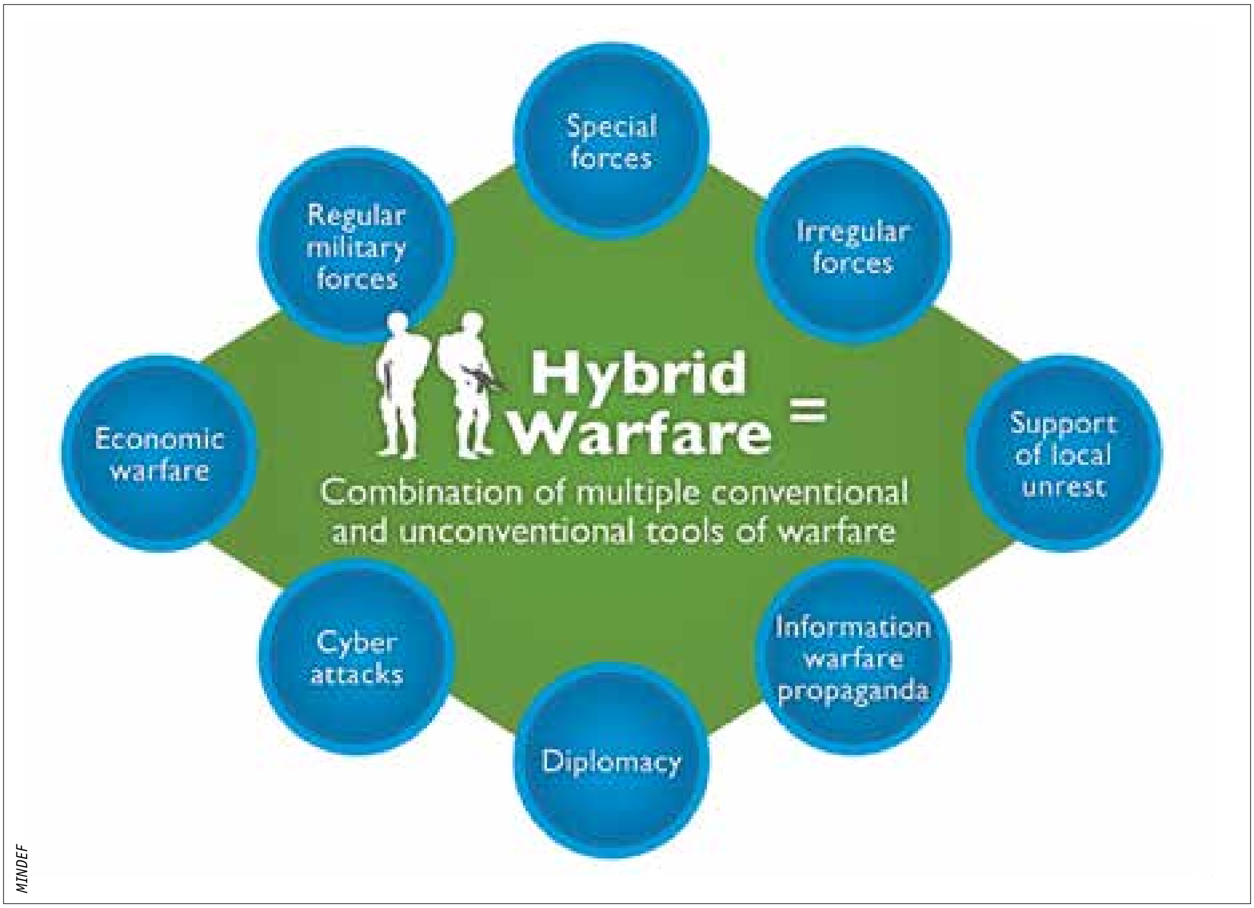


Figure 2: Dr Ng Eng Hen cited the recent unrest in Ukraine as an example of hybrid warfare, where subversion and subterfuge were conducted both through agents on the ground as well as through disinformation on social media

defines active cyber defence as its "synchronised, real-time capability to discover, detect, analyse and mitigate threats and vulnerabilities… It operates at network speed by using sensors, software and intelligence to detect and stop malicious activity before it can affect US DoD networks and systems."[20] Lynn highlighted that the active cyber defence approach would allow the Pentagon to build "layered and robust defences around military networks."[21]

Given the rise in advanced cyber attacks and the risks it poses to a state's national security, militaries around the world have evolved their cyber defence strategy to address the increasing threats.

As part of developing a comprehensive cyber defence approach, the Pentagon also inaugurated the US Cyber Command to "integrate cyber defence operations across the military."[22] The consolidation of cyber defence capabilities under one roof enabled the US Cyber Command to leverage on the government's intelligence capabilities to provide highly specialised active defences, such as detection and forensics, deception and attack termination.

Israel's Cyber Strategy

Similar to the US, Israel has also been a prime target for cyber attacks. During Operation Protective Edge in 2014, Israel faced large-scale cyber attacks on its civilian communications infrastructure via multiple DDoS and Domain Name System (DNS) attacks. The IDF's military communication networks were also targeted as part of the cyber attacks.[23] Senior Israeli security sources claimed that the attacks were traced to Iran and Qatar, key states that supported Hamas in the conflict against Israel.[24]

Given Israel's security environment and the increase in advanced cyber attacks, it has since developed a sophisticated cyber defence strategy that encompasses multi-faceted dimensions of cyber defence. A Policy Report on Israel's evolving cyber defence strategy states that:

> *"The IDF's strategy is… [focused on] developing unique interdisciplinary methodologies in a multidisciplinary national 'cyber-ecosystem' that integrates national research laboratories, military intelligence units, C4I organisations, the National Cyber Bureau, and start-up firms and entrepreneurs. In doing so, Israel is developing a "national cyber defence envelope" – a multi-layered cyber defence strategy leveraging automated computerised systems and highly-trained personnel that proactively combine intelligence, early warning, passive and active defence, and offensive capabilities across civil-military domains."*[25]

While there are no specific details and information about the IDF's cyber capabilities and operations from open sources, it is clear that much emphasis is placed by the IDF on active cyber defence, even to the extent of overtly mentioning offensive cyber capabilities in their menu of defences. In June 2015, the IDF announced that it would establish a new cyber command to lead all operational cyber activities, and it would be the fifth of such a branch directly subordinate to the Chief of Staff, other than the four existing Army, Air Force, Navy and Intelligence branches.[26] The establishment of this new organisation reflects the increasing importance of providing dedicated focus on integrating passive and active cyber capabilities in order to put in place a multi-layered cyber defence envelope.

The broad review of the US and Israel's national-level cyber defence strategies highlight that these states have embraced "a collaborative triptych of approaches to cyber security."[27] According to Robert Dewar, these approaches are not purely passive or active cyber defences; instead, a clearer categorisation of these measures would be to define them as fortified, resilient and active cyber defence.[28] These three pillars of cyber defence concept complement one another in providing a multi-layered and comprehensive cyber security approach. When combined, these strategies are able to address cyber threats ranging from low-level attacks (such as virus and DDoS attacks) to advanced cyber threats in the form of the next *Stuxne*t.

A COMPREHENSIVE CYBER DEFENCE STRATEGY FOR THE RSAF

In defining how the concepts of fortified, resilient and active cyber defences could be applied, we can draw parallels to key RSAF concepts and measures to identify the essential building blocks of an effective cyber defence framework.

As shown in *Figure 3*, passive and active cyber defence capabilities can be broadly categorised according to the nature of actions taken to defend against cyber threats. On one end of the continuum, there are passive defence mechanisms that serve to strengthen and fortify critical networks and infrastructures. In the middle of the continuum are cyber defence concepts that confer network resilience through responsive, adaptive, and occasionally deceptive actions to assure continued operations despite on-going attacks. At the most active end of cyber defence measures are proactive and active cyber defence operations that rely on well-researched threat intelligence.[29]

Fortification: 'Hardening' Our Infrastructure

Fortification of critical networks and infrastructures serves to reduce chances of a successful malicious attacks by preventing malicious access. This can take the form of installation of firewalls, encryptions and anti-virus software into operational systems and the supporting infrastructure, such as routers, network switches and computer software. Such forms of cyber

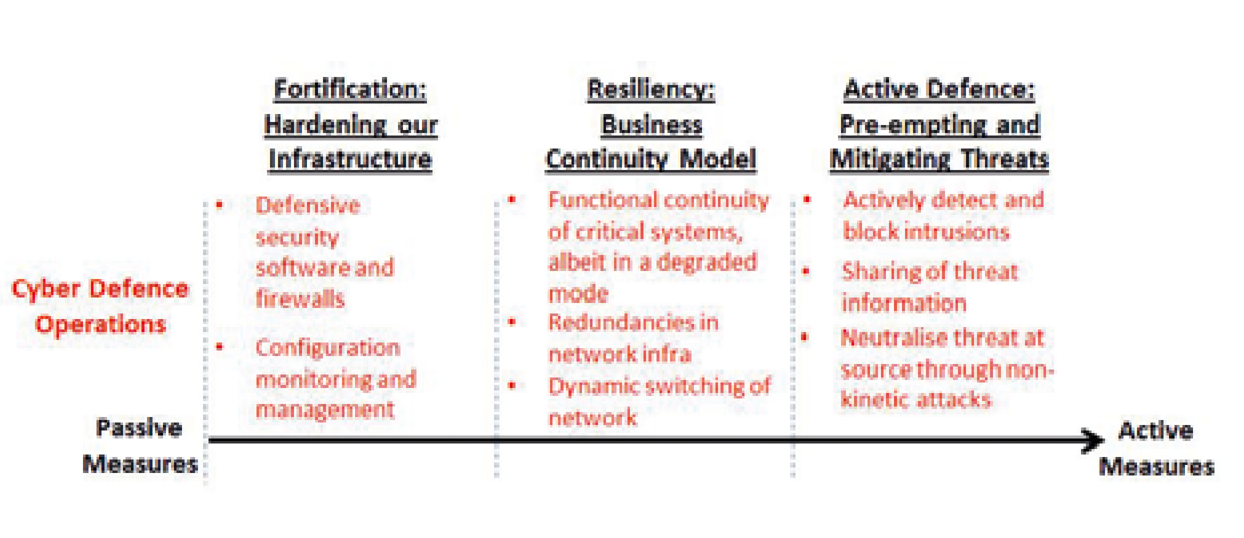

Fortification: Hardening our Infrastructure
Resiliency: Business Continuity Model
Active Defence: Pre-empting and Mitigating Threats
Cyber Defence Operations
• Defensive security software and firewalls
• Configuration monitoring and management
• Functional continuity of critical systems, albeit in a degraded mode
• Redundancies in network infra
• Dynamic switching of network
• Actively detect and block intrusions
• Sharing of threat information
• Neutralise threat at source through non-kinetic attacks
Passive Measures
Active Measures

Figure 3: Cyber defence concepts explained using Air Force Analogies

defence are akin to the hardening of our critical infrastructure against enemy air strikes, which is needed to protect our assets against external attacks.

Not surprisingly, many established militaries have recognised fortified cyber defence as one of the foundational pillars of cyber defence and have taken quick and extensive steps to establish cyber defensive perimeters to systematically secure communications and information networks.[30] Similar to the hardening of physical infrastructure, the implementation of cyber fortification across the entire organisation's network and computer systems can be costly and time-consuming. For example, a Task Force Report by the US Defence Science Board projected the investment cost for protecting the DoD's systems against low and mid-tier threats to be around US$50M to US$100M per year and would take around 18 months to complete.[31]

At the most active end of cyber defence measures are proactive and active cyber defence operations that rely on well-researched threat intelligence.

Fortification measures, though effective against novices and sporadic attacks, would eventually be defeated by determined and well-resourced attackers, especially when sophisticated attack techniques are employed to create new vulnerabilities in the systems, instead of merely exploiting existing security gaps. In addition, human errors, ignorance, wilful deviations from security protocols can often become the weakest link and provide determined attackers the much awaited opportunity to infiltrate our system to wreak havoc.[32] Overly-focusing our investments in fortification efforts will eventually yield diminishing returns in cyber defence effectiveness. Hence, we should adopt a balanced and pragmatic strategy by complementing our fortification efforts with a concept of cyber resilience, which would ensure sustained operational effectiveness in the face of cyber attacks.

Resiliency: Developing A Business Continuity Model

Resilient Cyber Defence is essentially about developing a business continuity model that focuses on survivability and functional continuity of the identified critical systems. In the event of a malicious attack or natural disruption to the system, a resilient cyber network will be able to prioritise its resources to ensure the provision of its primary service, albeit in a degraded mode.[33] For example, a power plant with a resilient cyber system encountering a cyber-breach will only suffer minor disruptions and still be able to produce a minimal but sufficient electrical output. Drawing a parallel to our Air Force, this is similar to our emphasis on robust air power generation through our investment in rapid runway repair capabilities to ensure a quick recovery of our air campaign after enemy air raids.

Embracing this concept of resilience is especially critical for the RSAF as it can provide the assurance of operational continuity in our centralised command and control of air operations by mitigating the impact of a successful cyber breach on the progress of air campaign. Simply put, building a resilient cyber system allows our commanders to continue with their orchestration of the air campaign with little or no degradation in their situational awareness or hindrance to their abilities in directing dispersed elements in the field and in the sky, even when a malicious cyber attack has taken place.

As part of this concept, it will be essential to establish a framework for the identification of critical systems that must incorporate high resiliency features, in addition to the systemic passive defence measures. In the operations phase, a highly competent crew of network experts must be able to accurately analyse and contain the operational impact of a successful cyber attack on the overall RSAF campaign.

This resilience concept proposes that in addition to providing agile and adaptive Command and Control, dynamic switching of network configuration reduces the chances of a successful 'target reconnaissance' by the adversary. In addition, incorporating decoys in the unused regions of our network space could further obfuscate any reconnaissance effort, thereby increasing the amount of resources required of the enemy for a successful cyber attack.[34] The incorporation of decoys also provides data points and insights into any malicious activities, which can be used to substantiate intelligence gathering efforts. Such intelligence will be crucial for beefing up cyber defence measures, and can also form the basis of more active cyber defence operations, as explained in succeeding paragraphs. To this end, the RSAF can closely partner the defence technology community to develop and incorporate such techniques into our existing network infrastructures.

Active Defence: Pre-Empting and Mitigating Threats

While fortified and resilient cyber defence are considered passive approaches that focus on defending our networks and making them more resilient to attacks, active cyber defence involves a broad range of proactive measures to mitigate threats. The fundamental concept of active cyber defence is to actively detect and mitigate the threat before it inflicts damage on its intended target.

Proactive actions can be taken to neutralise or mitigate threats in different ways. According to Dorothy Dennings, active cyber defence actions can be classified into four categories: sharing, collecting, blocking and pre-emptive.[35] First, sharing 'refers to actions that distribute threat information' to other parties so as to mitigate the effectiveness of the threat. In air defence operations, such actions are analogous to sharing information on missile or aircraft threats to other SAF entities outside our network so that we can collectively counter the threat.

The second category is collecting, which is to "take actions to acquire more information about the threat."[36] This would include measures such as deploying additional sensors to detect intrusions, or deploy 'white worms' that are similar to viruses that can search, collect information and subsequently destroy malicious software.[37] In air defence lingo, this would be analogous to mounting additional surveillance radars to a heightened alert state or sending out fighter aircraft to intercept, identify potential air threats and subsequently shoot these threats down.

The third category is blocking, which comprises actions taken to block suspicious software or activities from suspected hostile IP addresses. It would also include identifying, analysing and blocking software or traffic that displays abnormal behaviours or match specific threat signatures.[38] Such actions are akin to the Israeli's Iron Dome concept, where incoming aircraft or missile threats are shot down or prevented from hitting their intended targets.

The fourth category is pre-emptive actions, which is to 'neutralise or eliminate a source used in the attacks'.[39] For example, it could involve hacking back the computer that is initiating the attack, or it could involve shutting down hostile servers for a botnet. Other times, when intelligence gathering has provided sufficient evidence of pending malicious activities from an external source, it could mean a pre-emptive cyber attack to take down the server or computer even before it could launch an attack. This may neutralise or eliminate the cyber threat.

OUR PEOPLE: THE CRUCIAL LINK

Even as we continue to invest in technologies that fortify our networks, provide better resilience against malicious cyber attacks and develop active defence capabilities to mitigate threats, it is important to turn to our people—the crucial link in the larger cyber defence architecture. Much can be done to shape cultures and mindsets, train operational instincts and to be in tune with the realities of today's cyber operational environment and the opportunities and challenges that accompany it.

Even as we continue to invest in technologies that fortify our networks, provide better resilience against malicious cyber attacks and develop active defence capabilities to mitigate threats, it is important to turn to our people—the crucial link in the larger cyber defence architecture.

Our RSAF warfighters must recognise that the cyber space domain is as real and important as the air, land and sea domains. We must understand the limitations and fundamental assumptions of operating in the cyber space domain. For example, we must ensure that our RSAF warfighters are cognisant that in the contested cyber space environment, the intent and attribution of cyber threats may be difficult to ascertain. In addition, we can fortify or secure our networks, but adversaries will try to probe and they need only to be successful once to create an impact on our operations.[40] Moreover, we should see our networks not simply as support systems, but rather, to treat the entire network itself as a strategic weapon system.[41]

Shaping the organisational culture and our people's mindsets to align with this frame of thought is important, so that our warfighters see themselves as each being crucial elements and gatekeepers of a strategic weapon system. This is analogous to the RSAF Safety Culture, which was painstakingly built over the years to ensure that our personnel are imbued with a 'Safety First' mindset to enhance our operational effectiveness. Just as Safety is a personal, command and organisational responsibility, cyber security is the responsibility of each RSAF warfighter and at every level. A single point of failure has the potential to create devastating effects to the entire cyber network. We will need to safeguard our cyber space 24/7, just as how we constantly safeguard our airspace.

We can also do more to train our people to have the operational instincts to be effective in the cyber domain. For example, the United States Air Force (USAF) is incorporating the cyber domain at the tactical and operational levels at the Red Flag series of exercises to reflect the growing importance of cyber operations on the battlefield.[42] The USAF cyber teams that participated in the exercises are able to get hands-on training while exercising a variety of their cyber capabilities. They will target the adversary and their infrastructures to degrade their capabilities, as well as simultaneously defend critical infrastructures and networks.[43] The RSAF should similarly consider incorporating cyber elements as a staple in our key exercises. This not only hones our warfighters' operational instincts in the cyber domain, but also reflects the RSAF's organisational emphasis on the cyber space domain.

CONCLUSION

As the RSAF continues to modernise and advance technologically, our systems will increasingly depend on networks and System-of-Systems (SoS) capabilities to shorten the Observe, Orient, Decide and Act (OODA) loop to deliver airpower more decisively. Our networks will also be linked to other networks in the Army and Navy for better synergy in the air, land and sea campaigns.

However, just as technology and networks are enablers for enhanced Command and Control (C2) for the RSAF, they are also vulnerable to cyber attacks. With the increasing use of cyberspace as the fifth domain in military warfare, it is of paramount importance for the RSAF to continue to build up and strengthen our cyber defence capabilities, processes and competencies in accordance with a comprehensive cyber defence strategy.

While cyber defence strategies comprising fortified, resilient and active cyber defence are not new concepts, the methods and means to implement these strategies are continuously evolving in tandem with the sophistication of cyber threats. The RSAF and Singapore Armed Forces (SAF) will need to partner with Singapore's defence technology community to develop revolutionary innovations that can enhance Singapore's national security. Most importantly, we also need to shape our organisational culture and train our people to ensure that we are always vigilant against cyber attacks that may be employed as part of hybrid warfare.

ENDNOTES

1. Ng Eng Hen, Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2016, posted 8 Apr 2016, http://www.mindef.gov.sg/content/imindef/press_room/official_releases.sp.html.

2. Frank .G Hoffman, "Hybrid Warfare and Challenges," Joint Force Quarterly 52 (October 2009): 34-39, http://smallwarsjournal.com/documents/jfqhoffman.pdf.

3. Steven Bucci, "The Confluence of Cyber Crime and Terrorism," Lecture #1123 on National Security and Defence, The Heritage Foundation, last modified June 12, 2009, http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism.

4. For a brief introduction on the early years of cyber threats, see Andrew F. Krepinevich, Cyber Warfare: A Nuclear 'Option'? Center for Strategic and Budgetary Assessments (2012), 41-45.

5. For more information on how criminal groups use malware to commit cyber-crime, see Joseph Menn, Fatal System Error: The Hunt for the New Crime Lords who are Bringing Down the Internet, 1st ed. (New York: Public Affairs, 2010).

6. Alexander Klimburg, "Mobilising Cyber Power," Survival 53 (2011): 49, as referenced in "A Walk on the Dark Side," The Economist, 2007, accessed June 1, 2012, http://www.economist.com/node/972376.

7. Steven Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Journal of Strategic Security 4, no.2 (2011): 49-60, http://dx.doi.org/10.5038/1944-0472.4.2.3.

8. David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, posted January 6, 2011, http://smallwarsjournal.com/printpdf/10080.

9. Michael Raska, "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy," S. Rajaratnam School of International Studies, Nanyang Technological University (January 2015): 6, https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

10. Krepinevich, Fatal System Error, 5-6.

11. Ibid., 3.

12. Michael B. Kelley, "The Stuxnet Attack on Iran's Nuclear Plant was 'Far More Dangerous' than Previously Thought," Business Insider, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T&r=US&IR=T.

13. Lee Ferran, Alexander Marquardt and Colleen Curry, "Flame Cyber Attack: Israel Behind Largest Cyber Spy Weapon Ever?" ABC News, May 29, 2012, http://abcnews.go.com/Blotter/flame-cyber-attack-israel-largest-spy-weapon/story?id=16449339.

14. Nicholas Falliere, L. Omurchu and E Chien, "W32. Duqu: The precursor to the next Stuxnet," Symantec Security Response (November 2011), available at www.usenix.org/conference/leet12/workshop-program/presentation/chien.

15. The definition of Advanced Persistent Threat (APT) is taken from National Institute of Standards and Technology (NIST). See NIST, Managing Information Security Risk: Organization, Mission, and Information System View. SP 800-39, 2011, quoted in Ping Chen, Lieven Desmet and Christophe Huygens, "A Study on Advanced Persistent Threats," in IFIP International Conference on Communications and Multimedia Security (2014): 64, DOI: 10.10071978-3-602-44885-4_5.

16. Irving Lachow, Active Cyber Defence: A Framework for Policymakers, Policy Brief (Washington, DC: Center for North American Security, February 22, 2013): 2, http://www.cnas.org/publications/policy-briefs/active-cyber-defence-a-framework-for-policymakers#.V9f93_CGOM8.

17. Ibid.

18. Pierluigi Paganini, "Operation Dust Storm, Hackers Target Japanese Critical Infrastructure," Security Affairs, February 24, 2016, http://securityaffairs.co/wordpress/44749/cyber-crime/operation-dust-storm.html.

19. William J. Lynn, "Defining a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs 89,no. 5, (September/October 2010): 98, http://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

20. As defined by the US Department of Defence in Department of Defence Strategy for Operations in Cyberspace (July 2011), 7. See also Lachow, Active Cyber Defence, 2.

21. Lynn, "Defining a New Domain," 98.

22. Ibid.

23. Raska, "Confronting Cybersecurity Challenges," 5.

24. Lappin Yaakov, "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says," The Jerusalem Post, August 18, 2014, http://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-attack-on-Israel-senior-security-source-says-371339.

25. Raska, "Confronting Cybersecurity Challenges," 5.

26. Meir Elran and Gabi Siboni, "Establishing an IDF Cyber Command," The Institute for National Security Studies, Insight No. 719, July 8 2015, http://www.inss.org.il/index.aspx?id=4538&articleid=10007.

27. Robert S. Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence," in Cyber Conflict (CyCon 2014): 8, http://ieeexplore.ieee.org/document/6916392.

28. Ibid.

29. The spectrum of measures was adapted from Robert Lee's sliding scale of cyber security. See Robert M. Lee, The Sliding Scale of Cyber Security, SANS Analyst Whitepaper (August 2015), http://www.sans.org: https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240.

30. Carmen-Cristina Cirlig, Cyber Defence in the EU: Preparing for Cyber Warfare? European Parliament Think Tank, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

31. James R. Gosler and Lewis Von Thaer, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, (Washington DC: Department of Defence, Defence Science Board, 2013): 11-12.

32. Joanna Belbey, “The Weakest Link in Cybersecurity,” Forbes Online, February 27, 2015, http://www.forbes.com/sites/joannabelbey/2015/02/27/the-weakest-link-in-cybersecurity/#6ee205137410.

33. Dewar, “’Triptych of Cyber Security’,” 15-16.

34. Keith A. Repik, Defeating Adversary Network Intelligence Efforts with Active Cyber Defence Techniques, (Ohio: Department of Air Force Air University, Air Force Institute of Technology, 2008): 46

35. Dorothy E. Denning, “Framework and Principles for Active Cyber Defence,” Computers & Security 40 (2014): 4,http://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20 Cyber%20Defence%20-%2011Dec2013.pdf.

36. Ibid.

37. Dewar, “’Triptych of Cyber Security’,” 9.

38. Denning, Framework and Principles for Active Cyber Defence, 3-4.

39 Ibid, 5.

40. Henry Kenyon, “Air Force Embraces New Mindset for Cyber Warfare,” National Defence Industrial Association, January 31, 2011, https://defencesystems.com/articles/2011/01/31/air-force-cyber-command-ready-for-operations.aspx.

41. Ibid.

42. Joey Cheng, “Sign of the Times: Cyber's Bigger Role in Air Force's Red Flag,” Defence Systems, October 3, 2014, https://defencesystems.com/articles/2014/10/03/air-force-red-flag-cyber-domain.aspx.

43. Ibid.

LTC Anthony Wong is a fighter pilot by vocation and currently serving as a Branch Head. A recipient of the SAF Academic Scholarship (Military), LTC Wong graduated from the Australian Defence Force Academy and holds a Bachelor of Science in Chemistry from the University of New South Wales. He was also a recipient of the SAF Post graduate Award and holds a Master of Arts in Security Studies from the Naval Postgraduate School.

MAJ Christopher Eng is an AWO (GBAD) by vocation and is currently Head of New Media and Public Relations in Air Operations Department, Air Force Information Centre. He graduated from NUS with a Degree in Mechanical Engineering (Aeronautical) (Honours). He was previously Officer Commanding (OC) of 163 SQN.

CPT Ronald Loh Ming Yao is a helicopter pilot by vocation, and is currently a Staff Officer in Joint Operations Department. CPT Loh was a recipient of the SAF Merit Scholarship in 2009. He graduated from the University of Warwick with a Bachelors of Science in Economics, Politics, and International Studies (Hons, 1st Class), and subsequently from Columbia University with a Masters of Arts in Political Science.

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

Developing Key Competencies in the RSAF to Defend against Hybrid Warfare

by ME6 Spencer Goh, MAJ Joe Zhang, MAJ Tang Mun Bbun & CPT Rae Tan Yiwei

Abstract:

Singapore is a small country with open and intricate technological networks and as such, we are particularly susceptible to hybrid wars where military and non-military tools are employed in an integrated campaign to achieve surprise, seize the initiative and overcome a country. The authors highlight that in order to protect Singapore, the Singapore Armed Forces (SAF) should increase its focus on building the capabilities to counter the unconventional threats that are typically used in hybrid warfare. The essay focuses on the four typical domains within hybrid warfare namely, information, cyber, electronic and intelligence. They feel that these are the areas in which the RSAF must build on, in order to be able to defend Singapore by ensuring the attainment of air superiority and the provision of support for the SAF and whole-of-government efforts in hybrid warfare.

Keywords: Competencies, Develop, Hybrid Warfare, Human Resource, Operations

INTRODUCTION

During the Committee of Supply (COS) Debate 2015, Minister for Defence, Dr. Ng Eng Hen said that, "The SAF also has the need to re-make itself in response to a changing landscape from new security threats."[1] In his speech during the debate, he highlighted that "the very rules of war have changed" and that the SAF will have to transform in order to respond to evolving threats in hybrid warfare.[2] Hybrid warfare is a concept of warfare in which a multiplicity of state or non-state actors may employ both conventional and unconventional means in the peace-to-war continuum to achieve a political or ideological agenda.[3] The 2015 edition of Military Balance provides a very comprehensive definition of the latest manifestation of hybrid warfare, highlighting the methods employed, namely "the use of military and non-military tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilising diplomatic means; sophisticated and rapid Information, electronic and cyber operations; covert and occasionally overt military and Intelligence action; and economic pressure."[4]

In 2014, the world watched the annexation of Crimea as the Russians systematically took over Crimea from Ukraine through the successful conduct of hybrid warfare, involving the integrated use of cyber space and information operations, electronic warfare and irregular warfare. In addition, Ukraine's paralysis of their military option also played a part in their loss of Crimea. The paralysis began when Crimea's airspace was controlled by the Russians through mobile Surface-to-Air Missile (SAM) systems covertly deployed throughout Crimea. Exacerbating Ukraine's loss of Aerial Surveillance, Intelligence and Reconnaissance (AISR) capabilities was the inability to rapidly project forces into Crimea to seize or deny key communication infrastructures from falling into the adversaries' control. This resulted in the Russians having superiority in Information Operations as they controlled Crimea's cyber and electronic realms to mask illegal military actions, shaping the narratives to their advantage.

The Crimean crisis is especially relevant to Singapore and the SAF not only because it has shown that hybrid warfare is proliferating globally, but also because the crisis has shown that international agreements to protect a nation's sovereignty are not always guaranteed to work. For a small state like Singapore, it is precisely these international laws and agreements that help protect and advance Singapore's interests, both economically and militarily. However, regardless of the commitment of the international community to abide by these laws and agreements, there is still a degree of risk for potential aggression through the means of hybrid warfare as the domain of information, cyber, electronic and intelligence warfare are not defined by clear territorial boundaries like traditional warfare. Moreover, these laws and agreements do not necessarily include clear rules on the conduct of hybrid warfare against another country. As Singapore is a small country with open and intricate technological networks, we are particularly susceptible to such hybrid wars. In order to protect Singapore, the SAF should increase its focus on building the capabilities to counter unconventional threats that are typically used in hybrid warfare.

This essay focuses on four typical domains within hybrid warfare namely, information, cyber, electronic and intelligence. These are areas in which the RSAF

Wikipedia/Yuriy Lapitskiy

The Buk Missile System is one of the few SAM systems deployed by the Russians in the Crimean Conflict.

must build on, in order to be able to defend Singapore by ensuring the attainment of Air Superiority and the provision of support for the SAF and whole-of-government efforts in hybrid warfare.

The Crimean crisis is especially relevant to Singapore and the SAF not only because it has shown that hybrid warfare is proliferating globally, but also because the crisis has shown that international agreements to protect a nation's sovereignty are not always guaranteed to work.

INFORMATION-CYBER-ELECTRONIC-INTELLIGENCE DOMAINS AND THE RSAF

Information-Cyber-Electronic-Intelligence are typical domains of operations within hybrid warfare, aided by a multitude of technologies that exploit the same Electronic Magnetic Spectrum (EMS) in Cyber space, Air Space and even Outer Space. The ability to control or deny the adversaries' utilisation of EMS in these domains can critically cripple the adversaries' capabilities and potentially draw an end to hostilities. Achieving such an outcome will require us to utilise assets capable of seizing the initiative through speed, agility, covertness, persistency, long range and/or wide spread effect.[5] Hence, modern Air Forces with platforms capable of achieving superiority in the EMS are often employed for Information-Cyber-Electronic-Intelligence operations. For instance, had the Ukraine possessed the ability for ELINT aircraft to stay airborne for persistence intelligence gathering, they would have been able to detect the employment of Buk-M1 launcher in the Russian rebel-held territory in Donetsk and pin-point the responsibility to the Russian rebels. This EMS evidence would have limited the Russian's disinformation tactics aimed at derailing air crash investigators' efforts to hold the rebels responsible during the peak of the crisis. The Ukrainian government could have quickly stemmed the support for these Russian rebels in cyber space when fake reports of a Ukrainian Su-25 combat aircraft shooting down MH-17, or that the Buk launcher was actually located in Ukraine territories began to convolute the support for Ukraine's armed forces.

The ability to maintain a moral high ground in hybrid warfare is essential to maintain the support of local and international communities, thereby complementing the traditional force projection and hard physical target destruction that Air Forces undertake. Overt or covert adversaries may transmit news, propaganda and deceit through the internet, radio and television broadcasts, so as to influence a society and quickly derail support for states. The RSAF is usually the first responder in a full spectrum of operations from peace to war. As such, it is essential to manage information operations well to guard against potential use of news, propaganda and deceit by adversaries to derail public support of RSAF's operations.

The integrated use of Network-Centric system and Electronic Warfare system has proliferated in modern warfare. Like other modern Air Forces, the RSAF have to guard against such manipulation of the EMS in Cyber space, Air space and even Outer space, so as to ensure freedom of maneuver and the ability to counter potential attacks in the four domains within hybrid warfare. While these highly interconnected systems provide information fusion critical for Command and Control, a security breach in the integrity of these networks can cause delays to air operations. Hence, the RSAF has invested resources steadily over the years in cyber defence and electronic warfare capabilities to stay ahead of potential adversaries. The RSAF has also continuously invested resources in the Intelligence domain over the years as success of military operations increasingly depends on time criticality and accuracy of information.

Notwithstanding the RSAF's efforts in building capabilities to deal with the four domains of hybrid warfare over the years, more can be done to sharpen our overall capability so as to enhance our defence in hybrid warfare. Much has been done to advance our hardware to prepare the RSAF against hybrid warfare. To bring about the next bound of capability development against hybrid warfare, the RSAF should focus on the 'software', which is our people, as they are the key enablers of our hardware. The RSAF's combatants and first responders must possess a baseline competency to operate seamlessly in the Information-Cyber-Electronic-Intelligence domains in addition to their current vocational demands. In addition, there is also a need to Raise, Train and Sustain deeper expertise in a specialised pool of manpower in the RSAF who can anchor high-end capabilities to defend against hybrid warfare.

Baseline Competency for RSAF Personnel in Information-Cyber-Electronic-Intelligence Operations

Frontline combatants or first responders in the RSAF will not have the time to conduct detailed analysis or research during the conduct of the four domains of operations. Instead, efficient processes and protocols to maximise the effects of capabilities associated with these four domains are more important. This will require the ability to know and recognise possible techniques that an adversary can employ, and the ability to use their weapons or systems flexibly to gain an upper hand. Hence, the basic knowledge and skill sets associated with these four domains of operations can be emphasised at entry level when an RSAF personnel joins the service and progresses through the operational units.

Amidst the strategic human capital challenges such as low birth rate, ageing population, tighter labour supply, evolving aspirations and globalisation, there is a need to take a paradigm shift in how we Raise, Train & Sustain (RTS) our human capital to conduct the four domains of operations.

Deeper Expertise in the RSAF for Information-Cyber-Electronic-Intelligence Operations

Being competent and proficient at operating their vocational platforms (e.g. F16, Searcher and RBS-70) in the four domains will allow our people to ensure that the RSAF achieves mission success. At the same time, there is a need to support efforts in research and developmental work to attract and retain the brightest of the four domains of hybrid warfare in the force. Deep expertise will also provide the RSAF with the required capabilities to collaborate with partners in the design or testing of cutting edge technology thereby maintaining superiority in the four domains. Deeper expertise will also allow the RSAF to conduct in-house training especially where strict operational security is required.

RAISE, TRAIN, SUSTAIN HUMAN RESOURCES FOR INFO-CYBER-ELECTRONIC-INTELLIGENCE DOMAINS IN THE RSAF

Amidst the strategic human capital challenges such as low birth rate, ageing population, tighter labour supply, evolving aspirations and globalisation,

CPT Lim Chih Yuan (third from left), an RSAF Chinook pilot, briefing his crew on the day's mission just before take-off.

there is a need to take a paradigm shift in how we RTS our human capital to conduct the four domains of operations.[6] Without adding to the demands in recruitment, we will need to explore ways to nurture potential candidates and grow a core group of experts in the RSAF, who we will call 'Blackbelts', in these four domains. Ancillary measures will also have to be adopted to boost the RSAF's effectiveness in the four domains during periods when demands for these operations increase. This may be achieved by tapping the rest of the RSAF and possibly resources in the wider community, such as collaborating with public and private agencies. The essay will next examine how we can both RTS these 'Blackbelts' and the masses in the RSAF, as well as engage professionals in the public and private sectors to maintain our edge in these four domains.

Raising, Training and Sustaining the Masses and the 'Blackbelts'

The RSAF will need to grow a sufficiently sized talent pool in the Information-Cyber-Electronic-Intelligence operations through our pool of personnel who are already well-trained in their current vocations. Besides meaningful work, competitive remuneration and Route of Advancement (ROA) are key factors in encouraging RSAF personnel to adopt skills in the four domains, on top of their core vocations. As such, there could be additional incentives, such as accreditation (via competency or skill badges, or formal tie-ups with tertiary institutions), enhanced ROA and possibly skill-based allowances. This will encourage RSAF personnel from all vocations to pursue the various levels of qualification in any of the four domains. For instance, RSAF personnel can learn and get qualified to conduct one or up to two different operations. This will allow them to be employed in related fields in addition to their core vocations, leading to additional career pathways. This could be similar to the dual-vocation career of Air Intelligence Officers, where they can track along the Intelligence pathway or their core vocations in their ROA.

In order to develop a sufficiently large pool of personnel proficient in these areas, the RSAF will need to purposefully design training for the development of our people throughout their careers. Starting from the schoolhouses, a programme can be developed to raise the level of awareness and knowledge of our airmen on the four domains. Once deployed to their operational units, our airmen could be made to continuously handle practical aspects of these four domains of operations up to the intermediate level. As our airmen progress in the RSAF, there is a need to create modules in the various ROA courses, to continue to stimulate the interest and improve the knowledge of our people in these four areas. This can also expand to include professional courses conducted by industry experts, academia or even DSTA Academy.[7] Having short courses and providing hands-on work on Cyber, Electronics and associated operations may also pique the interest of in-service personnel to pursue higher level of qualifications in the four areas.[8]

While this strategy will be able to grow a sufficiently large workforce in the four domains of operations, we also need a core group of experts known as the 'Blackbelts' to anchor high-end development, planning and operations. These 'Blackbelts' will need to be identified as early as possible in their careers, when they show potential or interest in any of the four areas that they choose to pursue. In this regard, an Info-Cyber-Electronics-Intelligence agency could be instituted to manage this core group of talents. The talents should be part of the Military Domain Expert Scheme (MDES) as this will allow the RSAF to tap their skills over a longer career span. Once selected to be in this core group, the talents will track their ROA in the dedicated field of operations (i.e., either Info ops, Cyber, EW or Intel).

While the proposed strategy thus far could enable us to maintain a defensive edge against our potential aggressors in the four domains, we may need to look beyond our workforce to work with and tap on talents in the wider community.

Apart from identifying the potential 'Blackbelts' in the four domains, the earlier proposed Info-Cyber-Electronics-Intelligence agency can also be the Senior Specialist Staff Officer (SSSO) to plan and manage the career progression and deployment of manpower resources in these four areas. This will allow effective deployment of individuals at different stages of their careers with different levels of skills to drive the investigation, development and evaluation of hardware, software, techniques and capabilities in the four domains, across the whole RSAF.[9] This will ensure that the RSAF continues to maintain a pool of personnel proficient in performing baseline operations in the four areas so that when the need arises during peaks, such as during an onslaught of enemy info ops campaign on multiple fronts, the RSAF will be ready and able to quickly deploy our manpower to counter the attacks.

Leveraging on Resources beyond our Workforce

While the proposed strategy thus far could enable us to maintain a defensive edge against our potential aggressors in the four domains, we may need to look beyond our workforce to work with and tap on talents in the wider community. In a globalised world, sophisticated attacks in the four domains are no longer always developed by militaries. Increasingly, sophisticated attacks are designed by external experts and even hobbyists. Engaging the wider community will enable the RSAF to stay relevant and abreast of developments in the four areas outside of the military, in the private and public domains. This will then allow the RSAF to better prepare ourselves for threats in the four areas, and adopt best practices from the private and public domains.

The RSAF can consider engaging the services of professionals in the wider community on a freelance or contract basis to protect our interests and guard against any attacks in any of the four domains. Such a strategy to deal with ad-hoc threats in these four domains will not add permanent headcount with sunk costs for the RSAF. Some threats can be dealt with using permanent solutions, such as developing software to counter a particular malicious virus or code that is attacking our cyber security systems. In such a situation, the RSAF can offer one-off contracts to professional firms or individuals to develop permanent solutions such as software or enhance our cyber systems. While the RSAF already engages the services of professionals in the information domain through the use of advertising agencies for our recruitment drives, similar efforts could be considered for the other three areas of operations.

In the information operations domain, the RSAF already actively engages the traditional media, opening up slices of RSAF operations to journalists and reporters. The intent is to allow them to have a better understanding of the RSAF and address any misconceptions. With the rise of online and social media, the RSAF will need to proactively engage online citizens and social media users to debunk myths and misconceptions posted and shared online. We could first identify and engage prominent figures, bloggers and social media influencers who are familiar with, and positive towards the RSAF, so that they can act as the RSAF's advocates. The intent is to proactively bring differing viewpoints to the forefront, encourage fair and open discussions that may help to address untruths and possibly provide insights about the RSAF that not everyone in the public is aware.

Active engagement of the population can also be achieved through the organisation of competitions. For instance, the US recently organised the 'Hack the Pentagon Challenge', where it invited the larger community to report vulnerabilities without the fear of prosecution. Instead of only finding out about network security gaps after they have been compromised, such competitions allow organisations to discover network security gaps and adopt pre-emptive measures to counter any attacks. Competitions pertaining to information operations could also be organised for the general public, with prizes for those with the most Facebook likes for their stories on positive experiences in the RSAF's outreach events. Through these initiatives, we can engage the wider public and build their support for the RSAF.

DSTA

Champion team of the Polytechnic/University Category giving a demonstration to Permanent Secretary (Defence) Mr Chan Yeng Kit and DSTA's Chief Executive Tan Peng Yam on how to light up a smart light bulb using their laptop at the 2016 Cyber Defenders Discovery Camp.

Apart from competitions, the RSAF could also create awareness among the younger generation on the new skill-sets required in these four areas of operations. This will potentially enlarge the pool of interested candidates for such work in the longer term. For example, the recent Cyber Defenders Discovery Camp organised by DSTA could encourage students with cyber technological skill-sets or interest to consider work in MINDEF and the SAF.[10] In a similar vein, the RSAF can also review the Singapore Youth Flying Club (SYFC) and NCC-Air curriculum to include excerpts of these four domains during their early years of engagement. These students can potentially be tapped on as interns or attachment students to work in selected slices of the four domains. They may then be attracted to join the RSAF and pursue a career in these four domains.[11]

The importance of leveraging resources beyond our workforce in the RSAF cannot be emphasised more in the current context where battles are consistently taking place in the four areas without open declarations of war. It is essential that we continue to tap the expertise in the wider community while simultaneously engaging the public actively.

CONCLUSION

The operating environment and threats are continuously evolving and lines that once legalised a military option have become more difficult to define. The success of a state at defending against hybrid warfare is dependent on how fast and co-ordinated its Whole-of-Government approach is in dealing with the threats. The RSAF is poised to handle a full spectrum of operations from peace to war to defend the nation. Likewise, the RSAF will need to continue to build higher competencies in operations that can contribute to the state's success in defending itself against hybrid warfare. To this end, the RSAF should continue building competencies in the Info-Cyber-Electronics-Intelligence domain and develop an eco-system to RTS our human capital for deeper expertise in these four domains. Last but not least, we must not forget that there are resources beyond the RSAF that we can tap on to further strengthen the RSAF in these four areas.

ENDNOTES

1. Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2015, posted on 05 Mar 15 on the Official Releases, downloaded from https://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05Mar15_speech.html

2. Ibid.

3. Murray Williamson, Mansoor Peter.R, *Hybrid warfare: Fighting Complex Opponents from Ancient World to the Present*, New York : Cambridge University Press. 2012, pp. 292 - 296

4. James K. Wither, *Making Sense of Hybrid warfare*, Connections Q/15, no. 2 (2016):73-87

   Marian Radulescu, *Counter-Hybrid warfare. Developments and Ways of Counteracting Hybrid Threats/ War.* Downloaded from Proquest Military Collections

5. Myriam Dunn Cavelty, *Cyber Security, Contemporary Security Studies Third Edition*, Oxford University Press, Oxford, UK, 2013, pp 363-377

   MAJ Michael Scott, Information Operations, *Marine Corps Gazette*; Dec 2012; 96,12; Military Database

6. LTC Tee Pei Ling, MAJ Tjong Wei Chee, ME5 Wong Chong Wai, Human Capital Challenges for the RSAF, *Pointer: Beyond the Horizon: Forging the Future RSAF*

7. Major Schaap, Arie J, Cyber Warfare Operations: Development and use under International Law, *The Air Force Law Review;* 2009, pp121-173

8. Jim Tice, Push On to Spur Soldiers into EW, *Army Times*, May 23 2011

9. Electronic Warfare Warriors Defend the Digital Divide, US Fed News Service, Including US State News, Aug 2008

10. David J Kay, Terry J Pudas, Brett Young, Preparing the pipeline. The US Cyber Workforce in the Future. *Defense Horizons* 72 (Aug 2012): 1-15.

11. Marius Emil Patrichi, General Military Human Resource Management and Special Forces Human Resource Management. A comparative outlook. *Journal of Defense Resources Management*, Vol 6, Issue 2 (11)/2015.

ME6 Spencer Goh is an Air Force Engineer by vocation and is currently serving as Head, Logistics Planning Branch in the AELD. He was awarded the Local Study Award (Engineering) and graduated with a Bachelors of Engineering (Hons, 2nd Class) from NUS. ME6 Goh has held various positions in the bases and departments. He was Officer-in-Charge (OIC) Fire Control Flight in Air Logistics Squadron, Tengah Air Base, SO in Avionics Branch, Air Logistics Department, and OC of Avionics and Support Flight in Air Logistics Group – Fixed Wing 2. He also held the appointment of Head Air Force Recruitment Centre in Air Manpower Department, before attending the People's Liberation Army Air Force Command and Staff College in Beijing, China.

MAJ Joe Zhang is currently the CO of 122 SQN and was the Top Air Force Graduate in the 45th Command and Staff Course in 2014. He holds a Bachelor Degree of Electrical Engineering (Hons) from Nanyang Technological University.

MAJ Tang Mun Bbun is a AWO (GBAD) Officer and is currently managing NSmen as 'B' Battery Commander in the 18th Divisional Air Defence Battalion. He was previously a Staff Officer in Joint Manpower Department, managing manpower policies and resource allocation. He graduated from the Australian Defence Force Academy (ADFA) with a Bachelor of Arts (BA) in Indonesian Studies and BA (Hons, 2nd Class Upper) in Geography. He is able to write and speak Bahasa Indonesia fluently. As the top military and academic performer for his cohort in ADFA, he was awarded the Petro Ferdozcenko Bequest to conduct his Honours research overseas in Johannesburg, South Africa.

CPT Rae Tan Yiwei is an AWO (C3) by vocation, and is currently serving in the Air Intelligence Department. She was awarded the SAF Merit Scholarship (Women) in 2008, and graduated with a Masters of Arts in Business and Economics from the University of Edinburgh. Prior to her current appointment, she served as an AWO (C3) in 203 SQN.

NS50: Defending Singapore 50 Years and Beyond

by LTC Low Teck Loong, LTC Lee Kok Kiang, MAJ Nah Jinping & CPT Aaron Chan

Abstract:

In commemoration of the 50th anniversary of National Service (NS) this year, this essay traces briefly the origins of NS as a necessary response to the critical need of national security in newly-independent Singapore. The authors highlight that part of the success of the policy has been due to its evolution over the years to stay relevant to Singapore's society and meet our security needs. This has included building a strong NS training system, creating the Singapore Armed Forces Volunteer Corps (SAFVC), increasing opportunities for National Servicemen (NSmen) to contribute; easing administrative restrictions, improving recognition and benefits for NSmen, and encouraging community support for them. Lastly, the authors consider several possibilities of how the RSAF could tap on the NS resources in response to emerging threats in hybrid warfare, such as harnessing the current force and shaping the future, strengthening individual skills and knowledge, and strengthening partnership with the private sector and other ministries.

Keywords: National Service; Total Defence; Hybrid Warfare; Professional Trainings; Defence Partnerships

INTRODUCTION

Since the passing of the National Service (Amendment) Bill in 1967, every Singaporean male citizen is liable to be called up to serve NS upon turning 18. NS has played a big part in Singapore's success story. Indeed, without NS, we could not have built up the Singapore Armed Forces (SAF) and Home Team to protect ourselves from potential aggressors and the constantly evolving security threats. This essay celebrates 50 years of NS, and also aims to highlight several ways to continue to strengthen NS. Given the emerging threat of hybrid warfare, this essay also proposes possibilities that could be explored by the RSAF to enable our NSmen to make greater contributions in security and defence.

LOOKING BACK: THE GENESIS OF NS

When Singapore first became independent, the odds of survival were against us. Our strategic environment was dangerous and hostile. Back then, with no national defence force of our own, Singapore was defenceless and extremely vulnerable.[1] The painful memories of the Japanese Occupation and Indonesia's policy of *Konfrontasi* made defence an issue of survival. Our founding fathers quickly recognised the need to protect and defend our people and interests, if we wanted to shape our future. Given our small population and a lack of strategic depth, it was deemed that the only viable option was to build a defence force from citizen conscripts, who would be trained and led by a small group of regulars. In the event of an emergency, the whole nation could be mobilised to protect the country.

We have come far since the first 9,000 recruits were conscripted in 1967. It was not a popular move back then. The Chinese have a saying that good sons do not become soldiers, just as good iron is not made into nails. Hence, our founding fathers had to constantly emphasise the importance of NS. As then Defence Minister Dr Goh Keng Swee said, "Nothing creates loyalty and national consciousness more speedily and more thoroughly than participation in defence and membership of the armed forces."[2] This was not simply a military issue, but a national one. Members of Parliament back then, including Ong Pang Boon, Othman Wok, and Jek Yuen Tiong, joined the military to show that there was nothing wrong with being a soldier. It was a national priority to make NS acceptable to the masses. Through National Education efforts, the government gave conscripts a sense that what they were doing was important and meaningful, and convinced their parents that NS was important for Singapore's survival.

Today, many NSmen have become fathers, and their sons have served NS in turn. This has created strong and positive bonds, and continues to strengthen our commitment to defence. Also, the NS experience has evolved through the years. Compared to the past, NS recruits now have access to world-class training facilities and amenities, and are trained to use the latest weapons and equipment, and fight as an integrated unit.

Cyberpioneer

After a five-year hiatus, the Mobile Column returned to the National Day Parade Singapore 50 (SG50) celebrations, featuring nine families from the Singapore Armed Forces (SAF), Singapore Police Force (SPF),and Singapore Civil Defence Force (SCDF) comprising members who have served or are currently in service.

However, having the best hardware is not enough. What matters most is our Singapore spirit, which is essentially having the courage to stand up and the perseverance to carry on when the going gets tough, as well as the willingness to fight for our families, friends, and fellow Singaporeans. We have made NS a national institution and a defining part of the Singapore identity. We are determined to defend our home with our lives. Our NSmen are able to serve wholeheartedly, knowing that their families and employers continue to support NS strongly. This unity of purpose is crucial to SAF's deterrence, as it means that any potential aggressor will not only have to take on the SAF and Home Team, but also the entire Singapore population.

NS: SOUND PRINCIPLES SUPPORTING NATION BUILDING

NS was the only solution back then for us to form a defence force quickly, and this was a bold first step in our nation-building efforts. Choosing the right model to build our military force required careful consideration. Any country must consider the geopolitical landscape and raise an armed force that is able to handle the various types of conflicts they are most likely to face. In the case of conscription, it comes with a significant economic cost, and has a tremendous impact on civilian-military relations. However, Singapore's NS system has fared well with the strict adherence to three key principles.[3] First, NS must serve a critical national need, since it comes at a considerable cost to both the individual and the nation. This critical need is that of national security and our survival. The second principle is universality, which means all young able-bodied Singaporeans are conscripted. The third principle is equity, where all who serve NS are treated the same way, regardless of background or status. Through these principles, our NS system has been very successful.

> *"The nation-building aspect of defence will be more significant if its participation is spread over all strata of society."*
>
> *-Dr Goh Keng Swee*[4]

NS is important for involving the citizenry in the defence of Singapore. It serves as a strong force that integrates civilian and military bodies together for a single cause. This is anchored by a robust NS training system, comprising two years of full-time NS, followed by a ten-year Operationally Ready NS (ORNS) cycle. Through these training cycles, NSmen are updated on the latest technology and force multipliers, while gaining a deeper appreciation of what they do, and why NS is important. In addition, NS serves to integrate all Singaporeans across various social, ethnic, religious, language and cultural groups through the common experience of military training.[5] This creates a form of shared consciousness and identity among all Singaporeans, which is crucial in our social fabric. Another facet of Singapore that has the effect of rallying the society's support for security beyond the military domain is Total Defence, which calls for different segments of society to play a part in defending the nation. The concept of Total Defence comprises five pillars of defence: psychological, economic, civil, social and military. Such a strategy ensures that defence is not just the responsibility of the military alone, but that of the entire nation.

Our commitment to protect Singapore has given us over 50 years of peace and stability. Through its very existence and capabilities, the SAF has contributed significantly to the stable and peaceful security environment of our country. However, looking ahead, we must guard against complacency, for the nature of threats we face is constantly evolving. Increasingly, threats of a hybrid nature, including but not limiting to cyber warfare, low intensity conflicts and irregular or unconventional warfare, have manifested across various civil and military realms. Singapore's inherent vulnerability as a small island state remains unchanged, and we continue to need strong defence capabilities, as well as a strong and resilient citizenry.

Through its very existence and capabilities, the SAF has contributed significantly to the stable and peaceful security environment of our country. However, looking ahead, we must guard against complacency, for the nature of threats we face is constantly evolving.

STRENGTHENING NS

National Service has continuously evolved over the years to stay relevant to Singapore's society and meet our security needs. The defence of Singapore cannot lie solely on active regulars and servicemen. The SAF must also continuously maintain the professional competence of our NSmen. The establishment of the Committee to Strengthen NS (CSNS), chaired by Defence Minister Dr Ng Eng Hen, was set up in March 2013 precisely to explore and ensure the relevance of NS, and enable NS to better serve Singapore and Singaporeans.

CSNS spearheaded initiatives targeted at improving the NS structure and expanding community support for servicemen. The following paragraphs provide a brief summary of the implemented and on-going initiatives.[6]

A Strong NS Training System

The National Service structure has been improved by strengthening the NS training system through harnessing the existing pool of SAF, Singapore Police Force (SPF) and Singapore Civil Defence Force (SCDF) regulars who are equipped with the latest training methodology and technology. The addition of well-trained individuals to the training system will ensure that training is effective and safe, and that values will be inculcated effectively. The initiative will also increase the ratio of regular trainers to trainees across the SAF. From November 2016, pre-enlistees can indicate their choice of vocations, and the SAF will take into consideration an individual's skills,

MINDEF

Dr Ng Eng Hen chairing the fourth Committee to Strengthen NS (CSNS) Steering Committee at the Home Team Academy.

experience and vocation preference when deciding what vocation the serviceman is posted to. Our Full-time National Servicemen (NSFs) are likely to be more motivated to do their best with the enhanced matching between the individual's choice and organisational requirements, which could lead to a better NS experience for them.

SAF Volunteer Corps

The SAF Volunteer Corps (SAFVC) was established in October 2014 to give the wider Singapore community an opportunity to contribute to the defence of Singapore. The inaugural cohort of SAFVC marked the end of their basic training in June 2015. With the establishment of the SAFVC, women, first generation Permanent Residents (PRs) and new citizens can now contribute in areas such as legal, security, psychology and engineering.

Increasing Opportunities For NSmen To Contribute

While NSmen appreciate incentives that recognise their service, such incentives are not what drive long-serving NSmen. NSmen are contributing with greater satisfaction as they are increasingly being employed in operational, instructional and leadership roles. On top of that, through deliberate job matching, NSmen can be deployed more effectively. On the whole, the organisation benefits from increased NS contributions while NSmen can have a better NS experience through meaningful service.

Easing Administrative Restrictions

In order to create a positive NS experience, CSNS has looked into easing administrative restrictions throughout the entire National Service pipeline. For example, the percentage of pre-enlistees enlisted within four months after their post-secondary studies will be increased from 45% to 90%. This means that polytechnic graduates could have a shorter waiting time and start serving NS earlier. CSNS has also proposed ways to reduce the transition time between post-NS and tertiary studies.

In-camp Training (ICT) has also been made less cumbersome in several ways. First, NSmen are allowed the flexibility to use electronic and lifestyle devices in non-sensitive areas within camps during their ICT. Next, reporting requirements for exit control for NSmen was revised from the travel period of more than 24 hours but less than 6 months, to more than 14 days and less than 6 months. In other words, NSmen no longer have to notify the Ministry of Defence (MINDEF) of overseas trips lasting 14 days or fewer, instead of the previous 24-hour limit. Additionally, NS Relations Offices were established in the SCDF, SPF and SAF to facilitate NSmen with more complex administrative matters.

Recognition And Benefits For National Servicemen

National Servicemen have gained increased recognition and benefits through the revamp of the NS HOME (Housing, Medical and Education) which totals to a $15,000 subsidy over three service milestones applicable to supporting their education, housing and healthcare. Increased insurance coverage for our NSmen has also been implemented during their full-time NS and ICTs. For example, compared to the former SAF Group Term Life insurance scheme, the new scheme has seen an increase in areas of coverage for a lower premium. On top of that, the SAF has been working with the Workforce Development Agency to accredit soldering skills acquired during NS. This could increase employability and ease NSF's transition into the workforce. In addition, NSmen now receive $150,000 of insurance coverage while serving NS.

Encouraging Community Support For National Servicemen

CSNS proposed for community support to NSmen to be expanded in a multifaceted way. For example, awards such as the 'NS mark' will be given to companies with pro-NS policies. Such recognition may be considered for MINDEF/SAF contracts and hence would encourage companies to enforce good human resource practices that support NS. Next, facilities such as the Singapore Armed Forces Recreation Association (SAFRA) and HomeTeam National Service (HomeTeamNS) recreational facilities were extended not only to the servicemen, but also to their families. On top of that, families of servicemen will be recognised through the Family Recognition Voucher (FRV) scheme which was increased from the top 10% to top 30% of ICT performers. Furthermore, meaningful gifts are given to NSmen during significant stages of their life such as marriage or birth of a child. Finally, in order to enhance stakeholder engagement, the ACCORD (Advisory Council on Community Relations in Defence) was restructured and expanded to comprise (a) an Employer and Business Council; (b) an Educational Institutions Council; and (c) a Family and Community Council. These three new councils will actively reach out to their respective sectors of the community.

SAFEGUARDING OUR FUTURE WITH NS

We will next look at the possibilities of how the RSAF could tap on the NS resources to further strengthen our capabilities against the emerging threats in hybrid warfare, such as defence in cyber warfare. We believe that there are expertise in the domain of cyber warfare residing in the NS resources and can be tapped to build up the RSAF's capability in these domains quickly. Three initiatives that the RSAF could consider are: (a) Harnessing the current force and shaping the future; (b) Strengthening the individual's skills and knowledge; and (c) Strengthening partnership with private sectors and other ministries. Some of these initiatives may require NS policies to be adjusted at the MINDEF/SAF level.

Harnessing The Current Force And Shaping The Future

The NS system could be refined so that knowledge, skills and capabilities associated with identified domains in hybrid warfare could be better harnessed from our NS resources. In the previous section, we mentioned that pre-enlistees would get to indicate which vocations they would prefer to serve in, and the system would look at matching vocations and individuals' aptitude to their interest.[7] We can also explore another initiative where the RSAF pro-actively takes in pre-enlistees with the right skillsets in building up expertise in niche areas. This can be done by identifying pre-enlistees with the necessary academic background and arranging for them to fulfil their NS requirements in positions related to identified domains in hybrid warfare. For example, polytechnic graduates with an electronic engineering background could be earmarked to perform their NS in positions related to the employment of Electronic Warfare (EW) in the RSAF.

This idea can be extended to the NSmen resources as well. Every year, we have thousands of NSmen who continue to contribute to the RSAF through ICTs. Amongst them, some possess in-depth knowledge and are professionals in specific fields such as cyber security, corporate communications or engineering. Very often, NSmen with such talents are employed in general fields for their ICTs that do not give them the opportunity to contribute their civilian professional expertise. Through a re-vocation exercise, we can maximise the contributions of NSmen with niche capabilities. This can be done through identifying potential NSmen who fulfil our requirement based on their experience in relevant fields or qualifications. Once this group of people is identified, we can encourage them to join vocations that are relevant and can contribute more to hybrid warfare. By being able to make a difference, they may glean a much more positive experience from NS. We will have a win-win situation where the RSAF can be the choice organisation in attracting talent in addition to the regular workforce, while the identified pre-enlistees and NSmen can serve their NS in a vocation related to their expertise and interest, with opportunities to improve professionally.

We will have a win-win situation where the RSAF can be the choice organisation in attracting talent in addition to the regular workforce, while the identified pre-enlistees and NSmen can serve their NS in a vocation related to their expertise and interest, with opportunities to improve professionally.

Next, we can review the current MINDEF/SAF policy of determining the deployability of individuals. The aim is to expand the pool of human resources for NS and allow more Singaporeans to contribute in a more meaningful way. It will be timely to review the assessment of individuals' deployability and examine their potential to be employed in a selected field. This can be seen in the Israeli Defense Force (IDF).[8] Unit 9900, an intelligence unit from the Israeli Army, employs teens with autism in view that their heightened perceptual skills could contribute greatly to the intelligence work of the unit. In many militaries, teens with autism would have been exempted from service or could contribute in very limited areas. However, by identifying unique traits related to autism, the IDF has created additional ways for Israelis to contribute to their country. Such ideas can be explored for MINDEF/SAF to expand the pool of precious human resource, and at the same time, enlist more Singaporeans to contribute in defence, especially in niche capabilities.

In shaping the future, we can help NSFs preserve relevant skills and knowledge in the realm of hybrid warfare which they acquired in NS. One approach is to assist them in their transition to the specific workforce of the identified domains. This can be done through career fairs or partnerships with the private sector companies similar to the Enhanced Career Fairs introduced by MINDEF and the Ministry of Home Affairs (MHA) in November 2015.[9] This will not only allow the smooth transition of this niche group of NSFs into the workforce in specific domains, but also allow the NS system to maintain a pool of relevant expertise for future call-ups. In this manner, they can gain deep expertise in the selected domains and contribute meaningfully when they report back for ICT in the same domain. The SAF can also consider leveraging the Volunteer Corps (VC) platform to expand the pool of resources and tap the expertise from the private sectors. Possible initiatives can be to provide companies with certain privileges if their company's staff are part of the VC or if their NSmen are deployed in specialised domains.

Strengthening Individual Skills And Knowledge

After looking at widening and developing the specific pool of resources, we can explore possibilities where the skills and knowledge of NSFs and NSmen in specific fields enhanced and strengthened. This can be through improving the learning environment and strengthening the individual's deep learning cycle.

In order to stay relevant in the dynamic operating environment, NSFs and NSmen in these specific fields would be more committed and productive if they are could upgrade themselves during the ICTs. This could be done through attending personal upgrading courses, seminars or forums conducted by in-house trainers, and benefiting from the sharing of personal knowledge and experiences by NSmen on specific fields that are relevant to the RSAF. For example, NSmen serving as corporate communications specialists in the private sector could share their experiences during their ICTs on communication strategies through a learning day arrangement. This could help other NSmen widen their perspectives and better appreciate the challenges in relevant topics.

Besides in-house trainings, we can leverage on external institutions for professional trainings. For example, the Cyber Security Institute (CSI) was launched by Singtel with the aim to provide training and courses related to cyber security in April 2016.[10] We could explore extending these upgrading courses conducted by external professional institutions to NSmen during their ICT. NSmen could view ICTs as opportunity to upgrade, and see value in their time spent during ICTs. The logic is simple: if we strongly believe that NSmen play an important role in our fighting force, we should equip and train them with the necessary knowledge and skills. In this manner, their employers will not view their absence as a loss to the companies, but an opportunity to partner the SAF to continuously help their staff to upgrade. This will lead us to our third strategy, which is to strengthen our partnership with the private sector and other ministries.

Moving ahead, the RSAF could explore defence partnerships with private companies and external agencies such as the Ministry of Home Affairs and the Ministry of Communication and Information. We have to recognise the important role played by private companies in the specific fields related to hybrid warfare

Strengthening Partnership With The Private Sector And Other Ministries

Threats that exist in hybrid warfare are not limited to targeting the SAF or the RSAF. No agency

NS Portal

NS Mark: An accreditation scheme to recognise organisations that pledge their commitment to National Service and Total Defence.

NSFs celebrating the successful completion of Basic Military Training.

in Singapore can afford the resources or the expertise to fight against these threats in silos. We will need to strengthen our defence eco-system against such threats, as well as collaborate with other relevant agencies and companies to instill public confidence and our people's commitment to defend the nation. Moving ahead, the RSAF could explore defence partnerships with private companies and external agencies such as the Ministry of Home Affairs and the Ministry of Communication and Information. We have to recognise the important role played by private companies in the specific fields related to hybrid warfare. We should explore more opportunities to strengthen this partnership where there are mutual benefits to the RSAF and the companies. Possible means include attachments, internships or collaboration research programmes for selected individuals in the identified fields during their full time NS or ICTs for cross learning. One possible arrangement for such collaboration is the Singapore University of Technology and Design (SUTD) and the Singapore Technologies (ST) joint cyber security laboratory. Such arrangements will allow our NSFs and NSmen to widen their perspectives on various issues and gain new insights or trigger new initiatives on the ground.

We could consider similar initiatives for partnership with ministries and national agencies. For example, the Cyber Security Agency (CSA) is the leading body at the national level overseeing cyber security strategy, education and industry development. An initiative could be the sharing of human resources between CSA and the RSAF in the field of cyber defence to facilitate the sharing of knowledge and experience. We could also collaborate with CSA to establish partnerships with the other ministries.

CONCLUSION

The NS system has contributed greatly to the defence of Singapore and the shaping of the Singaporean identity. Since the birth of NS in 1967, NSFs and NSmen have participated in operations that we have termed as hybrid warfare in today's context. While the NS system has enabled the RSAF to achieve many milestones and significant achievements in the past 50 years, it is timely to explore new initiatives that will enable the NS system to continue to contribute to the RSAF in the future. This is important with the RSAF's mission extending into the realm of hybrid warfare, thereby bringing unique challenges that our current arrangement in the NS system may not be able to fully address. This essay suggests three areas which could enhance the contributions of NSFs and NSmen: (a) Harnessing the current force and shaping the future; (b) Strengthening the individual's skills and knowledge; and (c) Strengthening partnership with private sector and other ministries. While some of the initiatives are not new, they can bring value when applied effectively in the RSAF's context. These initiatives can enable the RSAF to gain knowledge and expertise quickly in key domains in hybrid warfare. In addition, by better tapping on NS resources, we can engender greater commitment to defence in the NSFs and NSmen as they contribute more significantly to the defence of Singapore in the next 50 years and beyond.

ENDNOTES

1. Ministry of Defence, *Speech by Prime Minister Lee Hsien Loong at the NS45 Commemoration Dinner at the Float@ Marina Bay*, 2012, https://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2012/22oct12_speech.html.
2. National Archives of Singapore, *Speech by the Minister of Defence, Dr. Goh Keng Swee, In Moving the Second Amendment Bill in the Singapore Parliament on Monday, 13th March, 1967,* http://www.nas.gov.sg/archivesonline/data/pdfdoc/PressR19670313b.pdf.
3. Ministry of Defence, *Round Up Reply by Minister for Defence Teo Chee Hean in Parliament*, 2006, https://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2006/16jan06_speech_html.
4. National Archives of Singapore, *Speech by the Minister of Defence, Dr. Goh Keng Swee, In Moving the Second Amendment Bill in the Singapore Parliament on Monday, 13th March, 1967,* http://www.nas.gov.sg/archivesonline/data/pdfdoc/PressR19670313b.pdf.
5. Conscription and Force Transformation by LTC Dan Yock Hau, *Pointer*, v._29, n._4, 2003.
6. Cyber Pioneer, *Strengthening NS: What These Changes Mean To You*, 2014, https://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2014/jul14_cs.html#.V9IUWVuGPIV.
7. Ministry of Defence, *Fact Sheet: Update on the Committee to Strengthen NS (CSNS) Initiatives: Vocation Matching & Launch of NS Mark*, 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2016/jun/30jun16_nr/30jun16_fs4.html.
8. The Atlantic, *The Israeli Army Unit that Recruits Teens with Autism*, 2016, http://www.theatlantic.com/health/archive/2016/01/israeli-army-autism/422850/.
9. Ministry of Defence, *Fact Sheet: CSNS Recommendation: Enhanced Career Fairs*, 2015, http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2015/jun/30jun15_nr/30jun15_fs3.html#.V0hTITFJmUk.
10. Singtel, *Singtel Launches First-of-its-Kind Cyber Security Institute in Asia Pacific to Hone Cyber Skills and Preparedness*, 2016. https://www.singtel.com/about-us/news-releases/singtel-launches-first-of-its-kind-cyber-security-institute-in-asia-pacific-t.html.

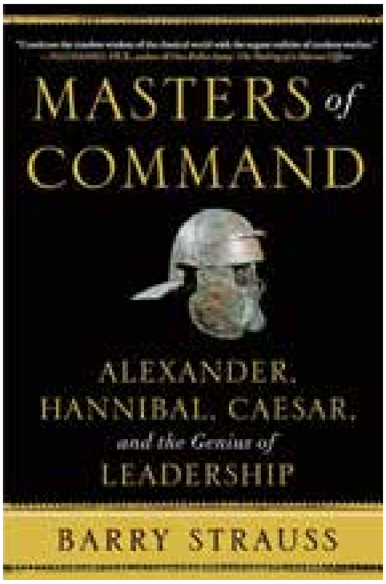
LTC Low Teck Loong is an AWO (C3) by vocation and is currently serving as the Deputy Commanding Officer in 111 SQN, Air Combat Command. LTC Low holds a Bachelors of Engineering (Mechanical & Production Engineering) and Masters of Science (Management) from the Nanyang Technological University (NTU). He graduated as the Distinguished Graduate from the 44th Goh Keng Swee Command and Staff Course.

LTC Lee Kok Kiang is an AWO (GBAD) by vocation and currently CO of 163 SQN. He holds a Bachelors in Mechanical Engineering (Honours) from NTU and a Masters of Science in Operations Research from Naval Postgraduate School. He graduated from the 45th Goh Keng Swee Command and Staff Course in 2014. His previous appointments include Branch Head of Defence Relations and Engagement Office (DREO) and S3 of 163 SQN.

MAJ Nah Jinping is a F-15 pilot and is currently Staff Officer (SO) of Air Weapons System Branch, Air Plans Department. She is a recipient of the SAF Merit Scholarship award and holds a Bachelors of Science (Honours) in Psychology from the University of Nottingham and a Masters of Arts in Educational Studies from the University of Michigan.

CPT Aaron Chan is currently serving as an SO in the Training and Development Branch, Defence Psychology Department. He was awarded the SAF Merit Scholarship in 2008. CPT Chan graduated from University College London (UCL) with a Bachelors of Science in Psychology (Hons, 1st Class) in 2011, and subsequently with a Masters of Science in Social Cognition (Distinction) in 2012.

Book Review



Barry Strauss, *Masters of Command: Alexander, Hannibal, Caesar, and the Genius of Leadership,* (New York: Simon & Schuster), 2012, 320 pages.

By **Jeria Kua**

INTRODUCTION

What do Alexander the Great, Hannibal Barca and Julius Caesar have in common? All were gifted battlefield commanders, skilled warriors and above all, exceptional leaders of men. Their legendary campaigns shaped the course of history indelibly, earning them the reputation of the ancient world's three greatest military commanders and duly attracting much scholarship on their illustrious careers. However, what Barry Strauss, Professor of History and Classics at Cornell University, has done differently in *Masters of Command: Alexander, Hannibal, Caesar and the Genius of Leadership* is to craft a concise and lucid comparative assessment of how the three generals waged, sustained and ended their famous wars of conquest. From their successes and failures in both the military and political spheres, Strauss distils the important lessons of leadership and strategic thinking still relevant to the modern context, both on and off the battlefield.

STRUCTURE AND STYLE OF WRITING

Strauss' treatment of the three figures is largely chronological, beginning with the build-up to their wars and ending with their deaths and legacies. He organises his book into five main chapters, each mirroring his 'five stage model of warfare.' In *attack*, he uncovers each commander's motivations for launching his campaign, with a common denominator of them being better off fighting than choosing to maintain the status quo. Guided by an overarching military and political strategy, all dealt a deadly first strike on the opposing army.[1] However, all faced *resistance*—an enemy counterattack that caused the invaders to stumble, pause and regroup. Through a combination of inspirational leadership and tactical errors made by their opponents, all three protagonists successfully rallied their armies and emerged victorious in a *clash*—a decisive battle that left them supreme and ready to *close the net* and finish the enemy off. Where all three fell short however was in *knowing when to stop*—the ability to end their conquests at the right time and in a way that would best allow them to consolidate their wartime gains.[2] None of them was therefore able to achieve his ultimate goal.

Strauss' style of writing also helps to enrich and enliven his analysis. He often begins his chapters *in medias res*, plunging readers into the thick of action and creating an atmosphere of suspense and excitement right from the start, truly making this book a page-turner. Although a plethora of battles is covered—unsurprising given the vast scale of all three wars—Strauss adroitly weaves them into the grand narrative, while the inclusion of maps, lively anecdotes and use of vivid language brings them to life and prevents his treatment of the three figures from turning dull. Filtering between each protagonist with consummate ease and clarity, he is able to maintain the flow of the narrative despite dealing with their campaigns separately.

THE TEN QUALITIES OF SUCCESSFUL COMMANDERS

Strauss' main goal in *Masters of Command* is, in essence, to extract the common characteristics displayed by Alexander, Hannibal and Caesar in their military careers, which he uses as a framework to compare, contrast and rate the three generals' performance as commanders at the end of each 'stage of war.' He narrows them down to ten particular qualities, ranging from ambition to leadership to even 'divine providence.' Finally, at the end of the book, he assesses their achievements holistically and crowns one of them as the 'greatest commander of ancient history.' Through learning from the great commanders' keys to success, Strauss seeks to offer both lessons and warnings "for leaders in many walks of life, from the war room to the boardroom."[3]

Firstly, all three commanders were hugely ambitious, combining the ability to dream big with a passionate, even overzealous drive to achieve them. Unlike Hannibal and Caesar, Alexander's war was fundamentally a war of aggression as he was in no immediate threat from Persia. He sought nothing but the complete conquest of the Persian Empire, even when signing a truce with King Darius III to end the war in 332 B.C. would have been more strategic. Hannibal was raised "(believing) in national greatness through war and empire," and sought to avenge Carthage's humiliation by Rome during the First Punic War.[4] Instead of choosing the safer option of defending what he already had, he decided to scare Rome into submission through conquest.[5] Not born into royalty, Caesar longed to be the "first man in Rome."[6] Gradually climbing the military ladder, he secured his place amongst history's finest generals by first conquering Gaul and later all of Rome during the civil war. Even that was not enough—he planned to defeat the Parthian empire, a feat he might have achieved if not for his death. Indeed, for the three commanders, a desire for greatness itself seemed to breed further success.

Coupled with a thirst for victory was an appetite for risk—the quality of audacity. They were bold in their plans and tactful in their decisions, making calculated risks when necessary and almost always emerged successful with the help of divine providence or luck. Despite being caught off-guard by King Darius' army during the Battle of Issus, Alexander immediately deployed his army for battle instead of retreating. He correctly gambled that his daring move would stun the enemy and scored an astonishing victory. In perhaps his most audacious move, Hannibal's army succeeded in completing one of the greatest and dangerous marches in the history of warfare by traversing the Alps on foot in winter, albeit at a massive cost. Expecting that Pompey's fleet would have its guard down, Caesar shipped his army across the Adriatic Sea from Brundisium in late autumn.[7] Without warships, he had his men transported in unarmed merchant ships, which could have easily been annihilated by the enemy. Overflowing in self-confidence and talent, the three were assured of their assessments of their opponents, and with the benefit of fortune on their side, reaped success. Perhaps more importantly, although they loved danger, they too knew precisely when not to take risks.

However, ambition and audacity alone do not make great commanders—good judgment and a sound grasp of strategy were essential for their plans to be successful. Alexander, Hannibal and Caesar all possessed exceptional strategic intuition on the battlefield. They remained resolute under pressure, learned from past experience and mistakes, correctly predicted their opponents' tactics and always planned ahead.[8] With a navy that could not hope to compete with Persia's, Alexander sought to overcome this weakness by conquering the enemy's Mediterranean seaports, halting Persia's ability to launch a naval offensive and forcing it to fight a land battle to his advantage. Hannibal was flexible in his tactics and was a master of the element of surprise, making full use of terrain and geography to launch ambushes on the Romans. In the Battle of Pharsalus, Caesar not only refused to fight Pompey in the hills where he would be disadvantaged, but also rearranged his battle order to adopt a new formation when he recognised his inferiority in cavalry, ultimately scoring a decisive victory. When faced with a problem, all three exercised superior foresight and intellect, and found a solution to overcome any setback.

Infrastructure forms the backbone of any army, and being capable of managing logistics with speed and agility was the hallmark of all three commanders. Although they usually found their army outnumbered, what they lacked in manpower was made up by superior organisation—they built up an experienced, synergistic combined-arms force unwaveringly loyal to its leader, and knew how to reorganise their forces swiftly in response to changing conditions.[9] Alexander developed his army around his strongest asset, the famed Companion Cavalry, which proved to be the cornerstone of his success during the war. In what was considered one of the greatest land battles in history, Hannibal was able to encircle the numerically-superior Romans in Cannae by strategically organising his troops in a crescent formation, scoring a decisive victory. While Caesar's legionaries were trained in pitched battles out in the field, he adapted them to the urban setting of Alexandria to pull off a successful siege. All three knew logistics at the back of their hands and were always on their toes, adapting to the fluidity of combat with speed and skill.

All three men recognised the importance of branding, and were willing to use terror as an instrument to enhance their reputation and enforce commitment to their cause. Alexander branded himself as the liberator of the Greeks from Persian rule, promising revenge for its invasion 150 years ago and the restoration of its former glory.[10] On the battlefield, he executed most Greek mercenaries fighting for Persia and destroyed Greek cities controlled by rebels as a warning to those who refused to side with him.[11] As winning the support of Italian cities was crucial to his war strategy, Hannibal asserted himself to be the new Hercules, promising freedom from Roman domination.[12] In defending his name, Caesar claimed to be the protector of the Roman way of life and concept of honour. His famous massacres in Gaul compelled many Italians to surrender to him promptly, while his famous policy of clemency won the hearts of many. The three leaders thus knew how to manipulate the emotions of the common people, instilling fear and showing mercy when it was to their advantage.

Perhaps the most important quality of a great commander is decisive, inspirational leadership—which all three generals certainly possessed in no small amount. Alexander did his best to keep Macedonian casualties low and rewards high, from pay to loot.[13] Sensitive to the mood of his troops, he always gave them adequate rest before major battles and provided reassurance when they lacked confidence, such as during the eclipse before the Battle of Gaugamela which they perceived to be an ill omen. Although his army was an assortment of different races, nationalities and languages ranging from the Celts to the Africans, Hannibal succeeded in keeping his army together for 15 years of constant fighting in enemy territory.[14] He never suffered a single mutiny, a testament to his exceptional leadership. For Caesar, even near the brink of defeat, he maintained the unity of his army and managed to withstand the near-starvation conditions of Dyrrachium in 48 B.C. and the gruelling long march that ensued.[15] On another occasion, he stopped a mutiny with a single word.[16] Sharing the same risks in battle as their men, the three generals led by example and knew how to connect with their men on a personal level. In return, they earned their soldiers' confidence, obedience and respect.

THE FAULTS IN OUR STARS

While the three commanders remain in the annals of history as prodigies of warfare, they were not without their shortcomings. Indeed, we have as much to learn from their failures as their successes.

Alexander performed exceedingly well at 'closing the net,' but did not understand when to stop. Drunk with success following his victory over Persia, he failed to consolidate his empire but instead pursued a number of unnecessary wars in the east, with little to no strategic value. Exhausted and homesick, his men mutinied and forced his return.[17] Furthermore, as king, Alexander failed to govern his territory or plan for a successor. As a result, his empire disintegrated upon his death and was carved up among his former generals. Unlike Alexander and Caesar, Hannibal's phenomenal victories on the battlefield, especially at Cannae, did not translate into success of his overall war strategy. He failed to deal a finishing blow on Rome, and instead gave time for his enemy to regroup and prepare a counterattack. The war dragged on beyond what he could handle, and wore down his men both physically and mentally. His defeat at the Battle of Zama dealt a finishing blow to his war of conquest. Much like Alexander, Caesar's successes left him a war addict and a victim of his own vanity. Although he made inroads in governing Rome, he was frustrated by politics and chose to escape reality by planning new wars elsewhere. Falling prey to delusions of omnipotence and invincibility, he failed to recognise the hostility brewing around him, and in his arrogance, dismissed his bodyguards.[18] He was thus left vulnerable to assassination by their former enemies.

From their examples, Strauss emphasises the importance of following up on victories in order to achieve overall mission success. He points out, "A victor's biggest mistake after winning a great battle is to expect success to fall into his lap. On the contrary, since necessity is the mother of invention, the vanquished are likely to be more ingenious than ever, and perhaps more dangerous."[19] In the end, overestimating themselves and underestimating their enemies led to the downfall of the three leaders.

CONCLUSION

In conclusion, Strauss has succeeded in elucidating the universal and timeless qualities of leadership from the examples of the true masters of command of ancient military history—Alexander, Hannibal, and Caesar. All were supreme battlefield tacticians, possessing both immense ambition and the willingness to take risks to succeed. Good judgement allowed them to adapt to change promptly. They all understood the importance of speed and logistics, and used fear as a means to enhance their reputation and legitimise their wars. They led inspirationally and earned the genuine respect of their men. Lastly, they were blessed with good fortune.

Although Strauss' admiration of the three figures is apparent, he maintains a balanced analysis throughout the book. All great heroes have flaws, and our protagonists are no exception. Hannibal was the worst of the three at long-term thinking, failing to capitalise on his decisive victory at Cannae to quash Rome. Alexander was so preoccupied with waging wars that he neglected governing his empire, which collapsed upon his death. Caesar was similarly prone to escapism, while his hubris ultimately proved to be his hamartia, leading to his death on the Ides of March. Caesar, however, came closest to combining military leadership with political statesmanship. Strauss duly crowns him as the greatest commander of antiquity.

However, the book might not suit everyone's tastes. The comparative nature of the analysis means that certain battles had to be truncated and some details glossed over to avoid distracting the reader from the main narrative. While evaluating the military careers of all three figures is by itself no mean feat, those desiring a more thorough analysis will have to look elsewhere.

Nevertheless, despite being a slim volume of 320 pages, *Masters of Command* is an excellent primer on three of the greatest generals in history and ought to be on the reading lists of both military history buffs and the casual reader. 🌎

ENDNOTES

1. Strauss, Barry, Masters of Command: Alexander, Hannibal, Caesar, and the Genius of Leadership, (*New York: Simon & Schuster*), 15.
2. Ibid.
3. Ibid., 5.
4. Ibid., 25.
5. Ibid., 26.
6. Ibid., 27.
7. Ibid., 98.
8. Ibid., 7.
9. Ibid., 11.
10. Ibid., 13.
11. Ibid., 12.
12. Ibid., 13.
13. Ibid., 238.
14. Ibid., 241.
15. Ibid., 247.
16. Ibid.
17. Ibid., 240.
18. Ibid., 247.
19. Ibid., 188-189.

William I, Prince of Orange (1533 - 1584)

by **Macalino Minjoot**

"Je Maintiendrai,"
(I will maintain)

-William the Silent[1]

INTRODUCTION

William I, Prince of Orange, also known as William the Silent or more commonly known as William of Orange, led the Dutch Revolt against the Spanish Habsburgs which sparked the Eighty Years War and eventually gained formal independence of the United Provinces in 1581.[2]

EARLY LIFE

William I was born on 24th April, 1533 in the castle of town Dillenburg in the duchy of Nassau in the Holy Roman Empire, now in Hesse, Germany. He was the eldest son, among his four other brothers and seven younger sisters, of William, Count of Nassau, and Juliana of Stolberg-Werningerode. Though his mother was raised a Roman Catholic, she eventually changed her religion twice, first to Lutheranism and then to Calvinism. Juliana was particularly close to William I. When he began his rebellion against Philip II of Spain, she supported her son morally and financially. Because of his mother's financial support, William was able to campaign against Spain in the Netherlands.

In 1544, his life changed completely when his childless uncle, René of Chalons, was killed during the Habsburg siege of the French town of Saint-Didier. As the last representative of the house of Nassau-Breda, Chalons had appointed his young nephew as his heir. The heritage included not only large possessions in the Netherlands, but also the Principality of Orange in southern France. From now on, William was no longer the son of an insignificant German Count, but a Prince.

Emperor Charles V (ruled 1519–1556) summoned the young boy from his family's castle at Dillenburg to the Netherlands, where he became a page at the Imperial court and was raised as a loyal and Catholic nobleman. The years that followed saw the remarkable transformation of the son of a Lutheran German count into a French-speaking Burgundian noble. Under the guidance of the regent, Mary of Hungary, William grew into a handsome young nobleman, elegant and well-spoken in French and Dutch as well as in his native German, intelligent and at ease with people.[3] William I was ready to serve the Habsburgs.

STRUGGLES WITH THE SPANISH EMPIRE

William came under the particular attention of the imperial family, and was very well-liked. He was then appointed a captain in the cavalry in 1551 and quickly rose up the ranks to command one of the Emperor's armies at an early age of 22. During the same year, the abdication of Emperor Charles V in favour of his son, Philip II of Spain, due to illness, would assure that William I would continue to assist them.[4] In 1559, William's political power greatly increased when Philip II appointed William stadholder (governor) of three provinces namely; Holland, Zeeland and Utrecht. A stadtholdership over Franche-Comté followed in 1561.[5]

Although William never directly opposed the Spanish King, he soon became the most prominent member amongst the opposition in the Council of State, together with Philip de Montmorency, Count of Hoorn, and Lamoral, Count of Egmont. They were mainly seeking more political power for themselves against the current government that was mainly ruled by Spaniards. William was also discontented with the increasing persecution of Protestants in the Netherlands. As mentioned, he was brought up a Lutheran and later a Catholic; William was religious but he supported the freedom of religion for all people. The Inquisition of the Netherlands, directed by the Cardinal Antoine Perrenot de Granvelle, increased opposition to Spanish rule among the then mostly Catholic population of the Netherlands.[6] Lastly, the opposition did not want the presence of the Spanish troops in the Netherlands.

After marrying a second time, it was assumed that William married Anne of Saxony to gain influence in Saxony. William found increasing confidence in his alliance with the Protestant princes of Germany following his second marriage. He began to openly criticise the King's anti-Protestant politics. In an iconic speech to the Council of State, William, to the shock of his audience, justified his conflict with Philip by saying that, even though he had decided to keep to the Catholic faith, he could not agree that monarchs should rule over the souls of their subjects and take from them their freedom of belief and religion.[7]

In the early 1565, a large group of noblemen, including William's younger brother, Louis, formed the Confederacy of Noblemen. On 5th April, they petitioned to end the Prosecution of Protestants. From August to October 1566, a wave of iconoclasm, the destruction of religious icons and other images or monuments for religious or political motives also known as Beeldenstorm, spread through the Low Countries. The Calvinists, which were mainly Protestant, and other forms of Christianity, such as Anabaptists, and Mennonites, were angered by the Catholic use of images of saints. In their eyes, it conflicted with the Second Commandment. Therefore, hundreds of statues in churches and monasteries were destroyed throughout the Netherlands.

Following Beeldenstorm, tensions in Netherlands grew and Margaret of Parma, governor of Netherlands, had to agree to the petition if the noblemen were to restore order to the Netherlands. However, Margaret did not fulfill her promise and soon several minor rebellions occurred which William was financially a part of. Following the announcement that Philip II, unhappy with the situation in the Netherlands, would dispatch his loyal general Fernando Álvarez de Toledo, Duke of Alba, to restore order, many Calvinists and Lutherans fled the country. William I also retreated to his native Nassau in April, 1567.

In August 1567, the Duke of Alba established the Council of Troubles, to judge those involved in the rebellion and the iconoclasm. William was declared an outlaw, and his properties were confiscated when he failed to appear for a summons before the Council. As one of the prominent figures in Netherlands, William I emerge as the leader of armed resistance. This armed resistance would raid coastal cities of the Netherlands, where they often killed Spanish and Dutch. William would also raise an army, consisting mostly of German mercenaries, to fight the Duke.

WAR

In October 1568, William led his army into the Duchy of Brabant, a state in the Holy Roman Empire. However, the Duke of Alba carefully avoided a decisive confrontation. The Duke expected William's army to fall apart quickly. As expected, disorder broke out in William's army as winter was approaching and they lacked resources. So, William was forced to turn back. He had several more plans to invade in the next few years, but the plans were not executed as he lacked the support and money.

However, it was largely as a result of William's leadership that the rebels overcame their differences and continued their military struggle, seizing the opportunities caused by the large-scale mutinies of the unpaid and unsupplied Spanish troops.

During 1571 to 1576, William and his army were slowly occupying towns in Holland and Zeeland where they were mostly in the hands of the rebels. Most notable was the capture of the city of Brielle by privateers, who had raised the Prince of Orange's Flag above the city, after the local Spanish garrison had left it unattended.[8] Together with the rebels, they almost captured the entire country. William then marched his army south where he won several more small battles. Eventually, Holland and Zeeland had to sign a treaty in 1576, the Pacification of Ghent.[9]

NETHERLANDS' INDEPENDENCE

When Don Juan signed the Perpetual Edict in February 1577, promising to comply with its conditions, the rebels felt that the war had been decided in their favour. The Calvinist rebels grew more radical, and attempted to forbid Catholicism in areas under their control. William was opposed to this both for personal and political reasons as he desired freedom of religion, and he also needed the support of the less radical Protestants and Catholics to reach his political goals. On 6th January 1579, several southern provinces, unhappy with William's radical following, signed the Treaty of Arras, in which they agreed to accept their Catholic governor, Alessandro Farnese, Duke of Parma (who had succeeded Don Juan) to rule the Netherlands.

The Duke of Parma was successful in reconquering most of the southern parts of the Netherlands because he agreed to remove all Spanish troops. Hence, the Netherlands finally had their own king.

In March 1580, Philip II issued a royal ban of outlawry against the Prince of Orange, promising a reward of 25,000 crowns to any man who would succeed in killing him. William responded with his Apology, a document in which his course of action was defended. However, Philip tortured the messenger so viciously that he restated his allegiance for the Protestant faith.

DEATH

Balthasar Gérard, a subject and supporter of Phillip II, regarded William of Orange a traitor to the king and to the catholic faith. When Gerard heard of the bounty of 25,000 crowns for the assassination of William, Gerard decided to travel to Netherlands to kill William.[10] Gérard went to the Duke to present his plans on killing William. The Duke was unimpressed but Gérard went ahead anyway.

Gérard presented himself to William as a French nobleman and gave him a precious seal of the Count of Mansfelt as proof.[11] However, William sent Gérald back to France to pass this seal to his French allies instead. Unfortunately, Gérard returned armed and on 10th July, Gerard made an appointment to meet William in his house in Delft. After his dinner with his guest Rombertus van Uylenburgh, Rombertus heard Gérard shoot William in the chest at close range with a handgun. According to Rombertus, William's last words were, "My God, have pity on my soul; my God, have pity on this poor people."[12] Even as he lay dying, William still had the plight of the people on his mind.

Even though Gérard fled immediately, he was unable to even escape the city of Delft. On 13th July, 1584, a scant 3 days after William' death, Balthasar Gérard was sentenced to be brutally executed—even by the standards of that time.[13] William I, Prince of Orange, holds the unfortunate record of being the first head of state to be assassinated by a handgun, and the second person to be killed by a firearm.[14] William was supposed to be buried with his ancestors in the city of Breda, but due to the war he was interred in the Protestant church of Nieuwe Kerk in Delft instead.[15] Since then, most descendants of the House of Orange-Nassau, including every member of the Dutch Royal Family, has been buried there.

CONCLUSION

William had never expected that such an important title would be thrust upon him at such a young age. While William fought for the freedom and independence of Netherlands with all his power and might, many regarded him as a traitor to his religion and principles. His aims were for the Netherlands to be independent of the Spanish empire, free from foreign intervention and for its people to have the freedom of belief and religion. William proved that he was indeed a capable leader who managed to unite both the merchants and rebels against the Spanish Habsburgs.

ENDNOTES

1. Kelley L. Ross, "Je Maintiendrai," The House of Orange and Nassau. http://www.friesian.com/ross/orange.htm.
2. United Provinces was the Dutch Republic in Europe that existed from 1581-1795 when they separated from Spanish Habsburg rule. It is one of earliest precursors to the modern Kingdom of Netherlands.
3. Biography. William the Silent Facts. http://biography.yourdictionary.com/william-the-silent
4. J. Thorold Rogers, The Story of Nations: Holland. London, 1889; Romein, J., and Romein-Verschoor, A. Erflaters van onze beschaving. Amsterdam 1938–1940. 150.
5. Wedgwood, C., William the Silent: William of Nassau, Prince of Orange, 1533–1584. (1944), 34.
6. Cardinal Granvelle was the leading minister to the Spanish Habsburgs.
7. "Prefigurations of the future? The views on the boundaries of Church and State of William of Orange and Viglius van Aytta (1565–1566)". A.A. McDonald and A.H. Huussen, *Scholarly environments: centres of learning and institutional contexts*, 1560–1960 (2004), 15–32.
8. Wedgwood, C., William the Silent: William of Nassau, Prince of Orange, 1533–1584. (1944), 120.
9 . They declared themselves ready to fight for the expulsion of Spanish troops together. However, they failed to achieve unity in matters of religion. Catholic cities and provinces would not allow freedom for the Calvinists.
10. "Mon Dieu, ayez pitié de mon âme; mon Dieu, ayez pitié de ce pauvre peuple." "De laatste woorden van prins Willem", Maatstaf 28 (1981), n._ 12. 67–100.
11. This seal would allow forgeries of the messages of Mansfelt to be made.
12. "Mon Dieu, ayez pitié de mon âme; mon Dieu, ayez pitié de ce pauvre peuple." "De laatste woorden van prins Willem", Maatstaf 28 (1981), n._ 12. 67–100.
13. Motley, John L. (1856). The Rise of the Dutch Republic, Vol. 3 http://www.gutenberg.org/cache/epub/4836/pg4836.html
14. Jardine, Lisa. (2005). The Awful End of Prince William the Silent: The First Assassination of a Head of State with a Hand-Gun.
15. New and Old Church of Delft http://oudeenieennieuwekerkdelft.nl/new-church/royal-family/william-of-orange?scope=14

Quotable Quotes

Our collective resolve and dedication to defend Singapore have earned us peace and stability.
– Goh Chok Tong (b. 1941), former Prime Minister and Emeritus Senior Minister of Singapore

Failures, repeated failures, are finger posts on the road to achievement. One fails forward toward success.
- C. S. Lewis (1898-1963), British novelist, poet

Never give up. Today is hard, tomorrow will be worse, but the day after tomorrow will be sunshine.
- Jack Ma (b. 1964), Chinese business magnate

Do the difficult things while they are easy and do the great things while they are small. A journey of a thousand miles must begin with a single step.
- Lao Tzu (600-531 BC), Chinese philosopher and founder of Taoism

When you have strict censorship of the internet, young students cannot receive a full education. Their view of the world is imbalanced. There can be no true discussion of the issues.
- Ai Weiwei (b. 1957), Chinese contemporary artist and activist

No cause justifies the deaths of innocent people.
- Albert Camus (1913-1960), French philosopher, author and journalist

The way to gain a good reputation is to endeavour to be what you desire to appear.
- Socrates (471-399 BC), Greek philosopher

The intelligent man who is proud of his intelligence is like the condemned man who is proud of his large cell.
- Simone Weil (1909-1943), French philosopher and political activist

When you are purposeful and you have a big passion (that you are pursuing), there is so much more that you are capable of. More than you think you can do.
- Bebe Teo (b. 1971), Country Director of Retail Group Singapore, Johnson & Johnson Pte Ltd

I hope everyone that is reading this is having a really good day. And if you are not, just know that in every new minute that passes you have an opportunity to change that.
- Gillian Leigh Anderson (b. 1968), American-British film actress, writer and activist

Never was anything great achieved without danger.
- Niccolo Machiavelli (1469-1527), Italian historian, politician, philosopher and writer

Mistakes are always forgivable, if one has the courage to admit them.
- Bruce Lee (1940-1973), Hong Kong and American actor and martial artist

The measure of a man is what he does with power.
- Plato (427-347 BC), Greek philosopher

We can do anything we want to if we stick to it long enough.
- Helen Keller (1880-1968), American author and political activist

Without passion you don't have energy, without energy you have nothing.
- Donald Trump (b. 1946), 45th President of the United States of America

The greatest deception men suffer is from their own opinions.
- Leonardo da Vinci (1452-1519), Italian polymath

Everything that is done in the world is done by hope.
- Martin Luther (1483-1546), German theologian and monk

Good order is the foundation of all things.
- Edmund Burke (1729-1797), Irish philosopher and statesman

Justice cannot be for one side alone, but must be for both.
- Eleanor Roosevelt (1884-1962), American politician, diplomat and activist

Love is not consolation. It is light.
- Friedrich Nietzsche (1844-1900), German philosopher

Your most unhappy customers are your greatest source of learning.
- Bill Gates (b. 1955), American business magnate, entrepreneur, investor, author, philanthropist and Co-founder of Mircosoft

Tomorrow belongs to those who can hear it coming.
- David Bowie (1947-2016), British singer, songwriter and actor

Success is not final, failure is not fatal: it is the courage to continue that counts.
- Winston Churchill (1874-1965), Britain's Prime Minister during World War II

Instructions for Authors

AIMS & SCOPE

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

SUBMISSION DEADLINES

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

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

SUBMISSION GUIDELINES

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

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

Article Topics

POINTER accepts contributions on the following topics:

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

Book Reviews

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

Viewpoints

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

Required Information

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

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

Submission of Manuscript

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

Article Length

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

ENDNOTE FORMAT

Author's Responsibilities

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

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

Endnotes

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

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

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

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

Books

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

For example:

> Tim Huxley, *Defending the Lion City: The Armed Forces of Singapore* (St Leonard, Australia: Allen & Unwin, 2000), 4.
>
> Huxley, *Defending the Lion City,* 4.
>
> Ibid., 4.
>
> Edward Timperlake, William C. Triplett and William II Triplet, *Red Dragon Rising: Communist China's Military Threat to America* (Columbia: Regnery Publishing, 1999), 34.

Articles in Periodicals

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

For example:

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

Articles in Books or Compiled Works

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

Articles in Newspapers

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

For example:

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

Online Sources

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

For example:

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

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

For example:

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

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

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

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

EDITORIAL ADDRESS

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

COPYRIGHT

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

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

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

REPRINTS

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

PLAGIARISM

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

POINTER

The Journal of the Singapore Armed Forces

ISSN 2017-3956