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

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.

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.