POINTER

JOURNAL OF THE SINGAPORE ARMED FORCES

Vol. 42 No. 4 [2016]

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© 2016 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. 42 No. 4 [2016]

contents

FEATURES

contents

BOOK REVIEW

PERSONALITY PROFILE

Editorial

We mark the end of 2016 with our final issue of the year, Pointer Vol. 42, No. 4. As we reflect on all that has happened this year, one thing is very clear to us – the need to be vigilant and alert, always ready to protect our country and defend our sovereignty. As our Minister for Defence, Dr Eng Eng Hen said: "But one constant remains, whether in 1966, 50 years ago, today, and I suspect 50 years hence. Threats will remain, because this is the nature of geo-politics as history teaches us. Today, it is the threat of extreme terrorists."[1]

The topics in the essays published in this issue cover a discussion on the evolution and development of The Five Power Defence Arrangements (FPDA) as well as a discourse on the rise of cyber power and the impact of information technology.

The essay entitled, 'The Five Power Arrangements: A Contemporary Assessment.' is by MAJ Pek Wee Kian. According to MAJ Pek, the FPDA came into being in 1971 as the third security arrangement involving Australia, New Zealand, Britain, Malaysia and Singapore. In his essay, MAJ Pek attempts to trace the evolution of the FPDA over the past forty five years. He examines the contemporary interests of each member state as well as the potential pitfalls and opportunities in the future. Finally, he assesses whether the FPDA will survive the next forty five years.

In the essay, 'Cyber Power – An Age of Perpetual Disruption', ME5 Calvin Seah Ser Thong makes an analysis of the importance and impact of cyber power. ME5 Seah highlights that since the introduction of the internet in the 1990s, the internet has been rapidly growing in terms of usage and that countries have to use the internet to their advantage as the world is moving to towards the cyber age. In his essay, ME5 Seah first defines the meaning of cyber power and explains why it is important in this day and age. Next, he briefly describes what perpetual disruption through cyber power is and how these attacks would affect the defence force of any country. Lastly, using examples of cyber threats that had happened in the last decade, ME5 Seah describes how the examples would result in perpetual disruption by cyber power. According to ME5 Seah, cyber threats are wide-spanning, accessible and boundary-less. In the final analysis, ME5 Seah feels that cyber threats have become the norm and will continue in an age of perpetual disruption.

ME5 Su Juncun's essay is entitled, 'Information Technology: Friend or Foe.' According to ME5 Su, Information Technology (IT) has advanced by leaps and bounds over the past few decades. ME5 Su examines the implications of the advancement of IT on Singapore and the Singapore Armed Forces (SAF). He begins by tracing the rapid growth of IT and along with it, the evolution of cyber warfare, which has opened up a new battlefield in the realm of cyber space and shown the capability to facilitate psychological operations and perception management. On the other hand, ME5 Su contends that IT has presented many new opportunities for the SAF to exploit, especially in the areas of learning and training, safety and administration and raising public awareness via social media platforms. By employing a combination of 'Quality' and 'Quantity' safety nets, ME5 Su feels that the SAF will be better able to counter cyber attacks, also reaping the many benefits of IT advancements to further enhance its effectiveness in defending the nation.

In this issue, we are also pleased to feature two papers which were presented at the Goh Keng Swee Command and Staff College (GKS CSC) Seminar 2015. Held at the SAFTI Military Institute from 8th to 9th October 2015, the GKS CSC Seminar was entitled 'The Role of Technology in the 21st Century Battle-Space' and jointly organised by GKS CSC, the S. Rajaratnam School of International Studies (RSIS) and the SAF-NTU Academy (SNA).

The first of these essays is entitled, 'The Role of the Military in Cyber Space: Civil-Military Relations and International Military Co-operation' and is by Ms Caitríona Heinl. In her essay, Ms Heinl highlights the significance of co-ordination that is key at both the national level within a state and between countries from a strategic and policy perspective for cyber-related issues. She considers several significant matters that arise in terms of the role of the military and civil-military co-ordination for cyber security. She also highlights a number of challenges in finding the right roles and responsibilities for the military in national cyber security and then focuses on military co-operation and dialogue. Finally, she analyses how to ensure that there are mechanisms to prevent further escalation when militaries are involved in managing these threats.

Dr Thomas X. Hammes' essay is entitled, 'Technologies Converge and Power Diffuses.' According to Dr Hammes, the convergence of dramatic improvements in the fields of robotics, artificial intelligence, materials, additive manufacturing and nano-energetics are dramatically changing the character of conflict in all domains. These developments will provide smaller powers—and even some individuals—with capabilities that used to be the preserve of major powers. According to Dr Hammes, this diffusion of power has major implications on the conduct of warfare and national strategy. This is because while massive investment in mature technology leads to only incremental improvement in capabilities, the proliferation of many small and smart weapons may simply overwhelm a few exceptionally capable and complex systems. Strategically, small nations will be able to afford effective anti-access/area denial (A2/AD) defences that can defend not only their territories, but also reach out to strike an invader's intermediate and home bases. They can generate many of the capabilities of the most expensive current systems at a fraction of the cost, which will drastically change the calculus of intervention. However, the critical military functions will remain—but how they will be accomplished will change. Dr Hammes feels that rather than investing everything in few, exquisite and very expensive systems, it makes more sense to explore augmenting them and, in time, replacing them with systems that conform to small, smart, and many.

We are pleased to announce that the Chief of Defence Force Essay Competition 2016/2017 is now open for participation. We would like to invite all our readers to take part in the competition. Details can be found on the POINTER website: **http://www.mindef.gov.sg/safti/pointer.**

At this juncture, POINTER would like to bid farewell to our Chairman of the POINTER Editorial Board, COL Ng Wai Kit as he retires from service. We wish to thank COL Ng for his support, advice and encouragement. POINTER has benefitted much from his insightful observations and on a wide variety of military subjects. We wish you all the very best in the next stage of your career as you hang up your uniform, Sir.

We also bit a fond farewell to CFC Delson Ong. We thank him for all his contributions and wish him the very best in his future endeavours. Finally, we would like to wish all our readers a Merry Christmas and a Happy New Year! Happy Holidays!

The POINTER Editorial Team

ENDNOTES

[1] https://www.mindef.gov.sg/imindef/press_room/details.html?name=27oct16_speech&date=2016-10-27#.WEYlk9J97IU

The Five Power Defence Arrangements: A Contemporary Assessment

by MAJ Pek Wee Kian

Abstract:

The Five Power Defence Arrangements (FPDA) came into being in 1971 as the third security arrangement involving Australia, New Zealand, Britain, Malaysia and Singapore. This essay will attempt to trace the evolution of the FPDA over the past forty five years. The author then examines the contemporary interests by each member state as well as potential pitfalls and opportunities in the future. He assesses whether the FPDA will survive the next forty five years.

Keywords: Evolution; Potential Pitfall; Opportunities; Survive; Agreement

INTRODUCTION

Predecessors of the FDPA: The ANZAM and AMDA

The genesis of the FPDA can be traced from the heritage of the British Commonwealth military presence during the colonial era. The Australia, New Zealand and Anglo-Malaya (ANZAM), the first of such security arrangements, saw the defence of Malaya through the period of communist insurgency often referred to as the 'Malayan Emergency (1948-1960)'.[1] With Malaya and Singapore seriously lacking indigenous defence capabilities, the presence of ANZAM provided an insurance against potential external aggression and internal security threats.

Following Malaya's independence in 1957, the *Anglo-Malayan Defence Agreement* (AMDA) replaced the ANZAM as a formal treaty underpinning the alliance. The AMDA was renamed *Anglo-Malaysian Defence Agreement* in 1963, when Malaysia was formed from the merger between the federated states, crown colony and North Borneo. Unhappy with the formation of Malaysia, then-Indonesian President Sukarno launched a series of low-level military confrontations against Malaysia (mainly Sarawak and Sabah) and Singapore. The period of '*Konfrontasi*' (Confrontation) lasted from 1963 to 1966 and saw the infiltration of armed Indonesian soldiers into Malaysia and Singapore to conduct skirmishes. In Singapore, multiple incidences of bomb blasts occurred, with the most serious occurring outside MacDonald House along Orchard Road. Over a hundred Commonwealth forces lost their lives for the defence of Malaysia.

Britain's 'East Of Suez' Policy

Shortly after the Confrontation, Britain's Labour Government rationalised its involvement in the Far East, and announced in January 1968 that it would withdraw its military forces from east of Suez by 1971. These took place in the backdrop of uncertainty and tensions in the region. Apart from the continued paranoia over Indonesia's desires on the region after its unsuccessful Confrontation attempts, there was tension between the newly separated Malaysia and Singapore. Not far from home, Vietnam was suspected of harbouring ambitions on the region. While not intentional, the withdrawal of the British would create a vacuum in the region, which then-Prime Minister of Singapore, Lee Kuan Yew believed could be "filled by Russia, China or anyone else".[2] Furthermore, with the air forces and navies of both the Singapore and Malaysian armed forces in the nascent stages of development, a huge gap in air defence capabilities was imminent.[3]

Formalising the Five Power Defence Arrangements

A series of Five Power Talks were conducted between the members to seek the best arrangements replacing the AMDA. The new British Conservative Government which took power in 1969 merely delayed the inevitable withdrawal. When Malaysia tried to cut a separate bilateral security arrangement with Australia, then-Prime Minister of Singapore Lee Kuan Yew reasoned that Singapore was a small country without strategic depth, and that any attack on Malaysia would also threaten Singapore.[4] It was later agreed that the FPDA should be predicated on the 'indivisibility' of defence of Malaysia and Singapore. Finally, under the terms of its founding Communiqué declared on 16th April, 1971, Australia, New Zealand, the United Kingdom (ANZUK), together with Malaysia and Singapore pledged:

> *"… in relation to the external defence of Malaysia and Singapore, that in the event of any form of armed attack externally organised or supported, or the threat of such attack against Malaysia or Singapore, their Governments would immediately consult together for the purpose of deciding what measures should be taken or separately in relation to such an attack or threat."*[5]

The communiqué was strategically worded to be a consultative forum. The FPDA was later formalised with a collection of bilateral Status of Forces Agreements (SOFAs), separately established by Malaysia and Singapore with each of the ANZUK countries. This was important, as a treaty would likely have provoked negative reactions from countries in the region. Nevertheless, sceptics doubted that the arrangements would survive on a consultative nature, and dismissed it as merely a temporary transitional arrangement to allow the British to relinquish their commitments east of Suez. [7]

The communiqué was strategically worded to be a consultative forum. The FPDA was later formalised with a collection of bilateral Status of Forces Agreements (SOFAs), separately established by Malaysia and Singapore with each of the ANZUK countries.

FPDA GOVERNANCE AND EXERCISES

As part of the agreement, the ministers agreed to set up a Joint Consultative Council (JCC) and an Air Defence Council (ADC). The JCC would 'provide a forum for regular consultation at the senior official level on matters relating to defence arrangements', and was attended by Permanent Secretaries or Secretary Generals of Malaysia and Singapore and the British, New Zealand and Australian High Commissioners.[8] The ADC comprises one senior representative from each of the signatories and is in charge of the Integrated Air Defence System (IADS) located in Butterworth, Malaysia, for the air defence of Malaysia and Singapore. In the first decade however, the FPDA only conducted a few exercises, and only four JCC meetings took place.[9] It was only in the 1980s that the FPDA was re-invigorated, when the notion of regular FPDA exercises was raised and instituted by then-Australian Prime Minister, Malcolm Fraser, with support from the other nations.

Established on 1st November, 1971, the FPDA framework covered the formation of the Integrated Air Defence System to be responsible for the air defence of Singapore and Malaysia.

The annual Air Defence Exercises (ADEXs) was gradually expanded to incorporate regular land and maritime exercises. In 1981, the FPDA's first annual land and maritime exercises, Exercise Platypus and Exercise Starfish were conducted. The FPDA continued to upgrade its regular exercises to incorporate submarine and electronic warfare elements.[10] Due to Singapore's lack of training space, land exercises were alternately hosted by Australia and New Zealand. This continued till Malaysia and Singapore hosted Exercise Kris Sakti and Exercise Lion Spirit respectively, on their own grounds in 1987 and 1989. In 1990, the land exercises were renamed Exercise Suman Warrior and held in rotation between the five countries.

The 15-year absence of the Royal Air Force was vindicated with its appearance for Exercise Lima Bersatu held in 1988, where the British made its largest contribution with an aircraft carrier. In that same year, the FPDA Defence Ministers agreed that a FPDA Defence Chief Conference (FDCC) should be held every two years and a FPDA Defence Ministers Meeting (FDMM) every three years.[11]

In 1990, the first FDMM was held in Kuala Lumpur, where the Ministers agreed to shift the focus of FPDA exercises from purely air defence to combined exercises. This resulted in the back to back conduct of the ADEXs and Exercise Starfish starting from 1991, before the exercises were combined into a single Exercise Flying Fish in 1997. In the second FDMM in 1994, the FPDA was restructured with the merger of the JCC and ADC into the single FPDA Consultative Council (FCC). The FCC was given the mandate to set policy guidelines and provide oversight and approval for FPDA activities including the scope and range of the exercises. The third FDMM In 1997 agreed that the FDCC should play a greater role in guiding the professional development of the FPDA exercises.[12]

The fourth FDMM in 2000 laid the foundation to what was said to be the greatest transformation in the history of the FPDA: the designation of the Integrated Air Defence System to the Integrated Area Defence System (IADS), to give greater emphasis on jointness.[13] As a result, long term plans for joint exercises were adopted and land exercises were integrated with Exercise Bersama Lima. In 2003, with the rising trend of asymmetric threats, the fifth FDMM agreed for FPDA exercises to incorporate serials to deal with terrorism, maritime security and humanitarian assistance and disaster relief (HADR).[14] This signalled a shift of FPDA exercises towards more non-conventionalism. The sixth FDMM in 2006 gathered in the shadow of the 2004 Boxing Day tsunami, which signaled a need for FPDA forces to take on greater roles in building capacity and enhancing inter-operability in HADR operations.[15] The inaugural Exercise Bersama Padu and Suman Warrior in that year involved maritime security and HADR elements following the Ministerial direction.

The eighth FDMM coincided with the 40th anniversary of the FPDA in 2011. A stock-take of the FPDA was conducted and the Ministers reaffirmed the key contributions by the FPDA to regional security, and committed to improve co-operation in non-conventional areas and explore capacity building in counter-proliferation.[16] The Ministers also

The Defence Ministers being briefed on Exercise Bersama Lima, a major FPDA joint exercise involving air, maritime and land forces, which Singapore hosted in 2011.

reaffirmed the strong commitment of their respective nations to the Arrangements. Most recently at the 9th FDMM in 2014, the Ministers affirmed the mutual benefits and professional value of FPDA exercises and agreed to further enhance its professional value.[17]

CONTEMPORARY ASSESSMENTS

Outlook

Some authors have opined that the FPDA had, against all odds, survived the poor prognosis by sceptics who doubted the viability of the arrangements.[18] Indeed, sceptics had dismissed the FPDA as a temporary transitional agreement to provide for the defence of Malaysia and Singapore until they are strong enough to defend themselves, and a sufficiently loose arrangement to allow the British to relinquish their responsibilities east of Suez.[19] Forty five years on, the FPDA has evolved and adapted well to the new security challenges of the day. To determine whether the FPDA will remain relevant in the future, it is pertinent to examine factors for its longevity and its contemporary relevance.

Psychological Deterrence

Since its inception, the FPDA had provided Malaysia and Singapore with a certain level of psychological deterrence.[20] Any potential aggressors would have to hazard a guess as to whether their attack would trigger the rest of the four nations. Besides, any attempts on Malaysia or Singapore would also likely draw the involvement of the United States (US), an ally of both Australia and the United Kingdom (UK).[21] In the earlier days before the Malaysian Armed Forces and the Singapore Armed Forces (SAF) were capable of establishing its own defence, this psychological deterrence had retrospectively appeared to be effective. Besides, while not a military alliance, the robust exercise regime of the FPDA exercises have helped to hone the interoperability of the five armed forces over time. An interoperable force was more likely to pose a greater deterrence than a make-shift coalition. Furthermore, with UK as a permanent member of the United Nations Security Council with veto power, maintaining ties with UK would no doubt be advantageous in any crisis.[22]

Since its inception, the FPDA had provided Malaysia and Singapore with a certain level of psychological deterrence. Any potential aggressors would have to hazard a guess as to whether their attack would trigger the rest of the four nations.

Enhancing Bilateral Relations

Besides the intended outcome of security, the five nations were able to reap both political and economic benefits from the FPDA. The enhancement of defence relations brought about by the FPDA inadvertently contributed to the warming of bilateral ties between the member states. One important outcome was that the FPDA acted as an additional channel for confidence building between Malaysia and Singapore, two countries with fractious moments in their history.[23] The FPDA also allowed both countries to take a multi-pronged approach to their bilateral relations with the other ANZUK states. The close defence ties between the member states also facilitated military to military co-operation, as evidenced by the support rendered by FPDA armed forces during the search for the missing Malaysian Airlines MH370 in March 2014.[24] The FPDA had also notably provided the foundation for co-operation between member states to respond to natural disasters as well as in United Nations peacekeeping operations such as in Timor-Leste and Bamiyan, Afghanistan.[25]

Complementing Multilateral Instruments

Many academics have also concluded that the FPDA complements multilateral instruments such as the Association of South East Asian Nations (ASEAN) and the ASEAN Regional Forum (ARF) in supporting regional peace and security.[26] The ASEAN Defence Ministers' Meeting (ADMM) focuses on confidence building, enhancing dialogue and practical co-operation between ASEAN militaries and defence establishments. The ADMM focuses on non-traditional security issues and lacks the defence component.[27] This is complemented by the FPDA, which retains its focus of conventional warfighting despite the inclusion of non-conventional elements.

SAFEGUARDING THE INTEGRITY OF ARRANGEMENTS

The FPDA's resistance to expansion had served to safeguard the integrity of the arrangements. Even though the issue of introducing new regional members such as Brunei or Thailand into the arrangements had been raised on various occasions, it had not been realised.[28] The addition of a new state into the FPDA would invariably bring along its historical baggage and disputes with other regional states, leading to new sets of potential complications to the consultative arrangements. With the successes of the FPDA so far, the five nations are likely to adopt the 'if it ain't broke' mentality, where such potential complications were unwelcomed.[29] As Malaysia's Prime Minister Datuk Seri Najib Tun Razak said in 2004 when he was Deputy Prime Minister and Defence Minister, the including of other countries "would mean a major departure from the concept of the FPDA ... and we are not ready for that."[30]

EXTRACTING PROFESSIONAL VALUE

The FPDA exercises have evolved and adapted to remain relevant. In the early days, the training and professional guidance provided by the more established ANZUK forces had helped sharpen the nascent conventional capabilities of the Royal Malaysian Air Force (RMAF) and the Republic of Singapore Air Force (RSAF).[31] As the military capabilities of the Southeast Asian members improved, the five nations gradually exercise as contemporaries and the ANZUK forces are able to extract more considerable professional training value.[32] In the current construct, the five nations continue to share their expertise in both conventional and non-conventional elements of security through regular exercises, courses and seminars. Exercises in recent years had also taken on the civil-military dimension, where the armed forces co-operate with civilian agencies such as Singapore's Immigration & Checkpoints Authority, Singapore Police Coast Guard, Maritime Port Authority, Customs, and the International Red Cross.[33] The introduction of counter-piracy, maritime security and HADR also allows the development of capacity to address non-traditional security threats that the FPDA nations face.

ASEAN : Maintaining Regional Security and Stability for and by the People"
MALAYSIA 2015
9th ASEAN DEFENCE MINISTERS' MEETING (9th ADMM)
16th MARCH 2015 | LANGKAWI, KEDAH, MALAYSIA
MINDEF

Minister for Defence Dr Ng Eng Hen (fourth from right) taking part in the ASEAN Wave at the opening of the 9th ASEAN Defence Ministers' Meeting.

The introduction of counter-piracy, maritime security and HADR also allows the development of capacity to address non-traditional security threats that the FPDA nations face.

STRATEGIC INTERESTS

Strategically, the five powers continue to see the importance of the FPDA. The ANZUK countries, like their Southeast Asian members, have strong interests in the freedom of Sea Lines of Communications (SLOCs) in the region.[34] For the UK, the FPDA has allowed it to maintain a legitimate presence in the Southeast Asian region, where it has both political and economic interests.[35] Its commitment to the FPDA had recently been demonstrated by the deployment of a destroyer and six Eurofighter Typhoons halfway across the globe to participate in Exercise Bersama Lima 2014.[36] The UK Defence Doctrine also continues to articulate the importance of FPDA in UK's collective security.[37] For Australia, the FPDA provided it with a forward presence at Butterworth Air Base where its Royal Australian Air Force (RAAF) P3 Orion aircraft conduct surveillance of the maritime approaches to Australia.[38] It also continues to staff the appointment of Commander IADS with a two-star Air Vice Marshall from the RAAF. For New Zealand, apart from the SLOCs, the FPDA and ADMM-Plus provided multilateral exercises for the New Zealand Defence Force.[39] The defence white papers of both Australia (2013) and New Zealand (2010) outline that the FPDA allows their strategic presence in Southeast Asia, and is a proven security architecture which help addresses contemporary security challenges.[40]

POTENTIAL PITFALLS

President Jokowi, For Or Against?

In the face of positive developments, the future of FPDA is possibly clouded by several uncertainties.

Firstly, as the FPDA was formed only shortly after the Confrontation with Indonesia, it had been viewed with varying degrees of suspicion by Indonesia. The Indonesian Foreign Minister Mochtar Kusuma-Atmadja had once suggested in 1990 to 'disband' the FPDA and replace it with a new three power defence arrangement between Indonesia, Malaysia and Singapore.[41] The new President Joko Widodo has yet to make any strong statements against the FPDA; whether he would adopt a peaceful, neutral or hostile stance towards the FPDA, remains an unknown. Given Indonesia's recent actions to assert its sovereignty, coupled with Jokowi's vision to establish Indonesia as a maritime power, it remains uncertain if the FPDA, especially with the retention of a conventional angle in its exercises, would sit well with the new Indonesian administration.[42]

Inclusion Of East Malaysia

Secondly, FPDA exercises had traditionally been held in the South China Sea near to Peninsula Malaysia and Singapore. The absence of the FPDA in East Malaysia remained apparent and it was not unconceivable that member states may start suggesting the conduct of exercises there for a fresh start. This move however, is fraught with potential complications. The IADS traditionally does not cover East Malaysia and extending FPDA exercises there would likely increase the amount of Malaysian airspace available to the other FPDA partners, something which Malaysia may not be agreeable to.[43] Extending the coverage to East Malaysia could also potentially implicate the FPDA in an unwanted Southeast Asian conflict should it arise.[44] The Philippines retains dormant claims over Sabah in East Malaysia, and Malaysia is also a claimant state in the Spratly Island disputes. Conducting conventional exercises in East Malaysia would invariably incur the sensitivities of Philippines, China, Indonesia (who shares the long border of Kalimantan with Malaysia) and even Brunei.

Rising Operational Costs vs Values Of Exercises

Thirdly, with all member states facing rising operational costs of exercising at large scales, FPDA exercises must continue to maintain its relevance and allow the five nations, particularly the extra-regional ANZUK countries, to derive 'value for money' for travelling the distances.[45] Should the value of exercises be depreciated due to any reasons in the future, it could become challenging for the extra-regional ANZUK armed forces to justify their continued involvement in the region. This could potentially unravel the Arrangements and undo the good works put in by the five nations over the years.

CONCLUSION

As Mr Peter Ho, Singapore's former Permanent Secretary of Defence has articulated, 'the FPDA is like a chameleon, constantly adapting to the changing environment. Its physical avatar — IADS — has transformed itself from an air defence system to an area defence system, the only standing multilateral defence system in the region. This must be a unique achievement for a loose consultative framework.'[46] The Arrangements had also survived because it has been responsive to the needs of all members and not just the powerful.[47] The five nations continue to demonstrate commitment to the FPDA because they understood the strategic contribution of the Arrangements towards regional security, and also derive value from their participation. Indeed, the FPDA remains a unique security arrangement in the region that is difficult to replicate in the current context. Moving ahead, there is a quiet confidence that the 'chameleon-like' adaptability and its principles of consensus building, equity and gradualism would afford it flexibility and capacity to negotiate its way in the next forty five years ahead.[48]

BIBLIOGRAPHY

Ang Cheng Guan, “Malaysia, Singapore, and the Road to the Five Power Defence Arrangements (FPDA), July 1970–November 1971,” War & Society, v._30, n._3, (2011): 207-225.

Lee, Kuan Yew. From Third World to First, The Singapore Story: 1965-2000. (The Straits Times Press, 2012).

Crowe, Allan. The 5 Power Defence Arrangements. (Kuala Lumpur: Percetakan Konta Sdn Berhad, 2001).

Ho, Peter. “FPDA at 40: Still Effective and Relevant.” RSIS Commentaries 179 (2011).

Chin, Kin Wah. The Defence of Malaysia and Singapore: The Transformation of a Security System 1957-1971. (Cambridge: Cambridge University Press, 1983).

Chin, Kin Wah. “The Five Power Defence Arrangements: Twenty Years After.” The Pacific Review, v._4, n._3, (1991).

FPDA, Communiqué issued at the conclusion of the Five Power Ministerial Meeting on the External Defence of Malaysia and Singapore, London, 1971.

Keating, Gavin. “The Five Power Defence Arrangements: A Case Study in Alliance Longevity,” Australian Defence Journal v._170, (2006), 48-59.

Ang, Wee Han. “Five Power Defence Arrangements: A Singapore Perspective.” Pointer, v._24, n._2, (1998).

Thayer, Carlyle A. “The Five Power Defence Arrangements: The Quiet Achiever.” Security Challenges, v._3, n._1, (2007): 79-96.

Thayer, Carlyle A. The Five Power Defence Arrangements at Forty. Singapore: Institute of Southeast Asian Studies, 2011.

Wan, Gail. “Five Powers to cooperate in humanitarian assistance.” Cyberpioneer, 2006. http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2006 /June/06jun06_news2.html#.VO3QsvmUfT8.

MINDEF. “Joint Press Statement on the 8th FPDA Defence Ministers’ Meeting (2011).” http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2011/nov/01nov11_nr /01nov11_statement.html#.VOm0UPmUfT8.

Chin, Kin Wah. The Five Power Defence Arrangements and AMDA. Singapore: Institute of Southeast Asian Studies - Occasional Paper 23, 1974.

Huxley, T. “Singapore and Malaysia: A Precarious Balance?”(The Pacific Review, 1991), v._4, n._3.

Rahmat, R. “UK prepared to deploy military assets to support FPDA in event of future Asia-Pacific crises, says foreign secretary.” IHS Jane's Navy International. http://www.janes.com/article/48537/uk-prepared-to-deploy-military-assets-to-support-fpda-in-event-of-future-asia-pacific-crises-says-foreign-secretary.

Sinclair, Paul. “Five Power Defence Arrangements: A New Zealand Perspective.” (CSS Strategic Background Paper, 2013), 9.

Bristow, D. “The Five Power Defence Arrangements: Southeast Asia’s Unknown Regional Security Organisation.” (Contemporary Southeast Asia, 2005), v._27, n._1.

Emmers, R. “The Role of the Five Power Defence Arrangements in the Southeast Asian Security Architecture.” (RSIS Working Paper, 2010), n._195.

Ric Casagrande, “The Five Power Defence Arrangements – Are They Still Relevant to Australia in the 1990s?” Working Paper n._17, Australian Defence Studies Centre, Australian Defence Force Academy (1993): 3.

Mak, J. N. “Directions for Greater Defence Co-operation.” Institute for Strategic and International Studies (1986).

Ball, D. “Building Blocks for Regional Security: An Australian Perspective on Confidence and Security Building Measures in the Asia–Pacific Region.” Canberra Papers on Strategy and Defence n._83, Strategic and Defence Studies Centre, Australian National University (1991): 73-74.

Khoo, H. S. “The Five Power Defence Arrangements: If it Ain’t Broke…” Pointer, v._26, n._4 (2000): 107-114.

Asmani, A. “Malaysia open to review of its scope.” (The Straits Times, 2004).

MINDEF. “Factsheet: About Exercise Bersama Padu 2006.” 2015. http://www.mindef. gov.sg/imindef/press_room/official_ releases/nr/2006/sep/07sep06_nr/07sep06_fs.html#.VO3aoPmUfT8.

Royal Navy. “Daring arrives in Singapore ahead of five nations exercise”. 2015. http://www.royalnavy.mod.uk/news-and-latest-activity/news/2013/october/31/131031-daring-arrives-in-singapore

Ministry of Defence, United Kingdom, “Joint Doctrine Publication 0-01 UK Defence Doctrine”, London, 2014, 5. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf

Singh, D. “The Five Power Defence Arrangements: A Quiet Achiever.” (The Straits Times, 2011).

Ministry of Defence, New Zealand, “Defence White Paper 2010”, Wellington, 2010. http://www.defence.govt.nz/reports-publications/defence-white-paper-2010/contents.html

Department of Defence, Australia, “Defence White Paper 2013”, Canberra, 2013. http://www.defence.gov.au/whitepaper/2013/.

“Indnesia sinks Vietnamese boats to stop illegal fishing,” (The Straits Times, 2014).

Kurlantzick, J. “Jokowi’s Maritime Doctrine and What It Means,” (The Diplomat, 2014).

Brett, N. J. "How Relevant is a "Revitalised" Five Power Defence Arrangement to Regional Security? A Regional Perspective, 1989–1995." BA Honours Thesis, University College, University of New South Wales, Canberra, 1995.

ENDNOTES

1. Ang Cheng Guan, "Malaysia, Singapore, and the Road to the Five Power Defence Arrangements (FPDA), July 1970–November 1971," War & Society, v._30, n._3, (2011): 209.

2. Lee Kuan Yew, From Third World to First, The Singapore Story: 1965-2000 (Singapore: The Straits Times Press, 2012), 62.

3. Allan Crowe, The 5 Power Defence Arrangements (Kuala Lumpur: Percetakan Konta Sdn Berhad, 2001), 9.

4. Peter Ho, "FPDA at 40: Still Effective and Relevant," RSIS Commentaries 179 (2011): 3.

5. Chin Kin Wah, The Defence of Malaysia and Singapore: The Transformation of a Security System 1957-1971 (Cambridge: Cambridge University Press, 1983), 176.

6. Peter Ho, "FPDA at 40: Still Effective and Relevant," RSIS Commentaries 179 (2011): 1.

7. Chin Kin Wah, "The Five Power Defence Arrangements: Twenty Years After," The Pacific Review, v._4, n._3 (1991): 193.

8. FPDA, Paragraph 6d to Communiqué issued at the conclusion of the Five Power Ministerial Meeting on the External Defence of Malaysia and Singapore, London, 15-16 April 1971.

9. Gavin Keating, "The Five Power Defence Arrangements: A Case Study in Alliance Longevity," Australian Defence Journal 170 (2006), 49.

10. Ang Wee Han, "Five Power Defence Arrangements: A Singapore Perspective," POINTER, v._24, n._2 (1998): 2.

11. Chin Kin Wah, "The Five Power Defence Arrangements: Twenty Years After," The Pacific Review, v._4, n._3, (1991): 201.

12. Carlyle A. Thayer, "The Five Power Defence Arrangements: The Quiet Achiever," Security Challenges, v._3, n._1, (2007): 87.

13. Ibid, 88.

14. Carlyle A. Thayer, The Five Power Defence Arrangements at Forty (Singapore: Institute of Southeast Asian Studies, 2011), 52.

15. Gail Wan, "Five Powers to cooperate in humanitarian assistance," Cyberpioneer, 2006, http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2006/June/06jun06_news2.html#.VO3QsvmUfT8.

16. MINDEF, "Joint Press Statement on the 8th FPDA Defence Ministers' Meeting (01 Nov 11)," http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2011/nov/01nov11_nr/01nov11 _statement.html#.VOm0UPmUfT8.

17. MINDEF, "9th FPDA Defence Ministers' Meeting," 2015, http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2014/jun/01jun14_nr2/01jun14_fs.html#.VO9OLvmUfT8

18. Chin Kin Wah, The Five Power Defence Arrangements and AMDA (Singapore: Institute of Southeast Asian Studies - Occasional Paper 23, 1974), 14–15.

19. Allan Crowe, The 5 Power Defence Arrangements (Kuala Lumpur: Percetakan Konta Sdn Berhad, 2001), 3.

20. Carlyle A. Thayer, "The Five Power Defence Arrangements: The Quiet Achiever," Security Challenges, v._3, n._1, (2007): 92.

21. Ang Wee Han, "Five Power Defence Arrangements: A Singapore Perspective," POINTER, v._24, n._2 (1998): 3.

22. Gavin Keating, "The Five Power Defence Arrangements: A Case Study in Alliance Longevity," Australian Defence Journal 170 (2006), 51.

23. Tim Huxley, "Singapore and Malaysia: A Precarious Balance?" (The Pacific Review, 1991) v._ 4, n._3, 207.

24. Ridzwan Rahmat, "UK prepared to deploy military assets to support FPDA in event of future Asia-Pacific crises, says foreign secretary," (IHS Jane's Navy International, 2015), http://www.janes.com/article/48537/uk-prepared-to-deploy-military-assets-to-support-fpda-in-event-of-future-asia-pacific-crises-says-foreign-secretary.

25. Paul Sinclair, "Five Power Defence Arrangements: A New Zealand Perspective," (CSS Strategic Background Paper 9, 2013): 3.

26. Damon Bristow, "The Five Power Defence Arrangements: Southeast Asia's Unknown Regional Security Organisation," Contemporary Southeast Asia, v._27, n._1 (2005): 17.

27. Ralf Emmers, "The Role of the Five Power Defence Arrangements in the Southeast Asian Security Architecture," RSIS Working Paper, n._195 (2010): 20.

28. Ric Casagrande, "The Five Power Defence Arrangements – Are They Still Relevant to Australia in the 1990s?" Working Paper n._17, Australian Defence Stu ealand, "Defence White Paper 2010", Wellington, November 2010, p. 10., and Department of Defence, Australia, "Defence White Paper 2013", Canberra, 59.

29. Khoo How San, "The Five Power Defence Arrangements: If it Ain't Broke…," *POINTER*, v._26, n._4 (2000): 107.

30. Asmani, A., "Malaysia open to review of its scope," (*The Straits Times*, 2004).

31. Ang Wee Han, "Five Power Defence Arrangements: A Singapore Perspective," *POINTER*, v._24, n._2 (1998): 3.

32. Allan Crowe, *The 5 Power Defence Arrangements* (Kuala Lumpur: Percetakan Konta Sdn Berhad, 2001), 54-55.

33. *MINDEF*, "Factsheet: About Exercise Bersama Padu 2006," 2015, http://www.mindef. gov.sg/imindef/press_room/official_releases/nr/2006/sep/07sep06_nr/07sep06_fs.html#.VO3aoPmUfT8.

34. Carlyle A. Thayer, "The Five Power Defence Arrangements: The Quiet Achiever," Security Challenges, v._3, n._1 (2007): 65.

35. Gavin Keating, "The Five Power Defence Arrangements: A Case Study in Alliance Longevity," *Australian Defence Journal* 170 (2006), 51.

36. "Daring arrives in Singapore ahead of five nations exercise", Royal Navy, 2015, http://www.royalnavy.mod.uk/news-and-latest-activity/news/2013/october/31/131031-daring-arrives-in-singapore

37. Ministry of Defence, United Kingdom, *Joint Doctrine Publication 0-01 UK Defence Doctrine*, London, 2014, 5.

38. Daljit Singh, "The Five Power Defence Arrangements: A Quiet Achiever," (*The Straits Times*, 2011).

39. Paul Sinclair, "Five Power Defence Arrangements: A New Zealand Perspective," (*CSS Strategic Background Paper* 9, 2013): 3.

40. Ministry of Defence, New Zealand, "Defence White Paper 2010", Wellington, November 2010, p. 10., and Department of Defence, Australia, "Defence White Paper 2013", Canberra, May 2013, p. 59.

41. Chin Kin Wah, The Five Power Defence Arrangements and AMDA (Singapore: Institute of Southeast Asian Studies - Occasional Paper 23, 1974), 201.

42. "Indonesia sinks Vietnamese boats to stop illegal fishing," (**The Straits Times**, 20140. Joshua Kurlantzick, "Jokowi's Maritime Doctrine and What It Means," (The Diplomat, 2014).

43. Natalie J. Brett, "How Relevant is a "Revitalised" Five Power Defence Arrangement to Regional Security? A Regional Perspective, 1989–1995," (BA Honours Thesis, University of New South Wales, Canberra, 1995): 42.

44. Gavin Keating, "The Five Power Defence Arrangements: A Case Study in Alliance Longevity," *Australian Defence Journal* 170 (2006), 53.

45. Carlyle A. Thayer, "The Five Power Defence Arrangements: The Quiet Achiever," Security Challenges, v._3, n._1, (2007): 95.

46. Peter Ho, "FPDA at 40: Still Effective and Relevant," *RSIS Commentaries* 179 (2011): 3.

47. Gavin Keating, "The Five Power Defence Arrangements: A Case Study in Alliance Longevity," *Australian Defence Journal* 170 (2006), 53.

48. Allan Crowe, *The 5 Power Defence Arrangements* (Kuala Lumpur: Percetakan Konta Sdn Berhad, 2001), 14.

MAJ Pek Wee Kian is an Air Warfare Officer (Ground Based Air Defence) by vocation and currently a Staff Officer in Joint Research Department. MAJ Pek is a recipient of the SAF Academic Scholarship and holds a Masters of Chemistry (1st Class Honours) from Durham University, United Kingdom.

Cyber Power – An Age of Perpetual Disruption

by ME5 Calvin Seah Ser Thong

Abstract:

Since the introduction of the internet in the 1990s, the internet has been rapidly growing in terms of usage. This would also mean that countries have to use the internet to their advantage as the world is moving to towards the cyber age. In this essay, the author first defines the meaning of cyber power and explains why it is important in this day and age. Next, the author briefly describes what perpetual disruption through cyber power is and how these attacks would affect the defence force of any country. Lastly, using examples of cyber threats that happened in the last decade, the author describes how the examples would result in perpetual disruption by cyber power. Based on the author, cyber threats are wide-spanning, accessible and boundary-less, and cyber threats have become the norm and will continue in an age of perpetual disruption.

Keywords: Cyber Age; Perpetual Disruption; National Security; Information; Warfare

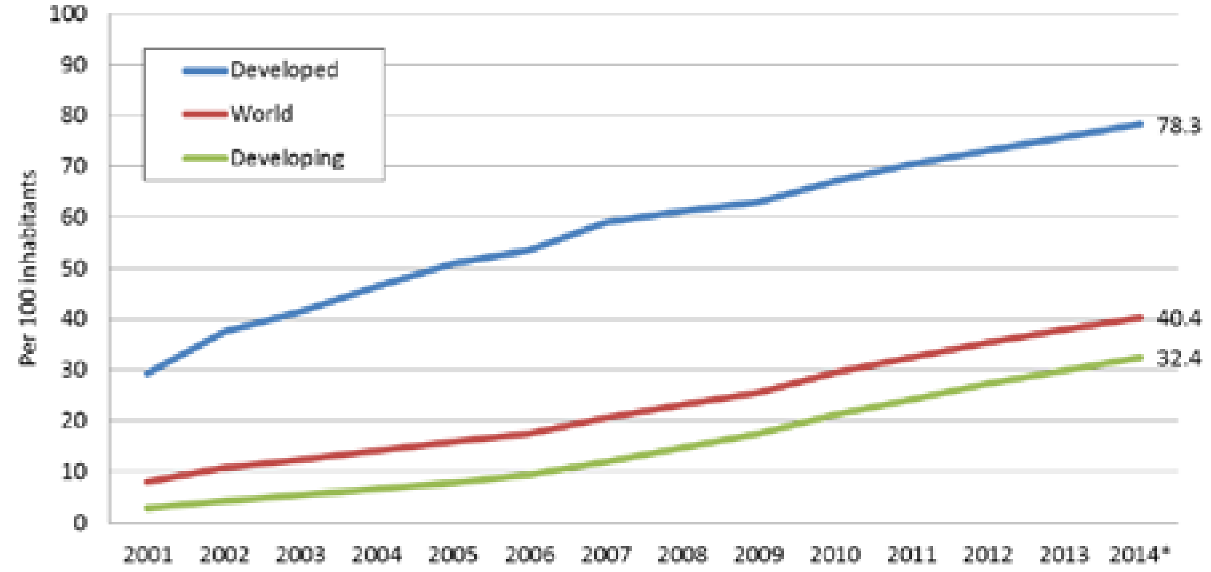
INTRODUCTION

> *"The very technologies that empower us to lead and create also empower those who would disrupt and destroy."*
>
> *– United States (US) Department of Defence (DoD) 2010 National Security Strategy*[1]

The internet is a medium that has grown rapidly; usage has increased from 16 million to 3.035 billion users presently since it was created to interconnect laboratories engaged in government research in the 1960s.[2] It has become the universal source of information for people all over the world and has inadvertently become a domain for a new kind of warfare termed cyber war which is war protracted by cyber means or cyber power. With cyber threats like the Stuxnet Worm that appeared to target Iran's nuclear programme, governments around the world have been called to arms to deal with this new threat. Some have even claimed that cyber power is making the Clausewitzean paradigm of war 'outdated' and 'ever more irrelevant'.[3] In 2011, the US DoD even recognised cyber space as an 'operational domain' in which its forces will be trained to respond to using traditional military force.[4] This is in addition to the four operational domains of air, land, sea and space.

In the 'The Rise of Cyber Power,' John Sheldon mentions that some scholars believe that the ease of cyber attacks "... heralds an age of perpetual disruption."[5] This essay thus explores the legitimacy of this claim. I will first discuss the domain of cyber space and then define what cyber power means. Next, I will discuss the possible reasons why cyber power is used and define what perpetual disruption by cyber power entails. I will then highlight examples of cyber threats that have been perpetrated through the use of cyber power. Following that, I will discuss the potential reasons and conclude why cyber power will indeed herald the arrival of an age of perpetual disruption.

Individuals using the Internet per 100 inhabitants, 2001-2014



The developed/developing country classifications are based on the UN M49, see: http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html

Note: * Estimate

Source: ITU World Telecommunication /ICT Indicators database

Figure 1: Internet users' continual growth[6]

THE DOMAIN OF CYBER SPACE

So, what is the domain of cyber space that cyber attacks are perpetrated from? The term was first coined by William Gibson in a short story in the July 1982 edition of the now-defunct science fiction magazine, Omni.[7] The term has since evolved and there are a plethora of definitions to define it. One of the definitions is that, "cyber space is a global domain within the information environment… framed by the use of electronics to… exploit information via interdependent and interconnected networks using information-communication technologies."[8] Simply put, cyber space can be thought of as the global nexus by which individuals and organisations share information and interact.

While it has experienced phenomenal growth, cyber space modestly started in 1969 when the US DoD started a connection of four computers to link universities and research centres. This was followed by the creation of transmission protocols in 1972 to enable the exchange of digital information. The database for the conversion of complex internet Protocol names to human-friendly Domain names followed in 1983, and the World Wide Web began in 1989. The incessant increase of users has seen the proliferation of cyber space into everyday products such as cell phones as well as objects typically not associated with cyber space, such as home appliances. The interconnectivity of cyber space has indeed transcended into one that is connecting all facades of our life as illustrated in *Figure 2*. While connectivity has been advantageous for us, it is this same connectivity in which much vulnerability has spewed from.[9] Such vulnerabilities have resulted from weaknesses in technology as well as improper implementation and oversight of technological products.[10]

Figure 2. Interconnectivity of the Cyber Domain[11]

DEFINING CYBER POWER

It has been argued that the success of the internet is what has transformed it into a potential domain for warfare, and as cyber space becomes more critical to a nation's economy, prosperity and national security, the more appealing to adversaries is the prospect of incapacitating it.[12] Through the use of cyber means, there have been many kinds of malicious actions that have been protracted including criminal acts to espionage as well as cyber attacks which may be carried out by nations, organisations or individuals. This wide spectrum of cyber threats and corresponding level of danger posed is depicted in *Figure 3*.[13]

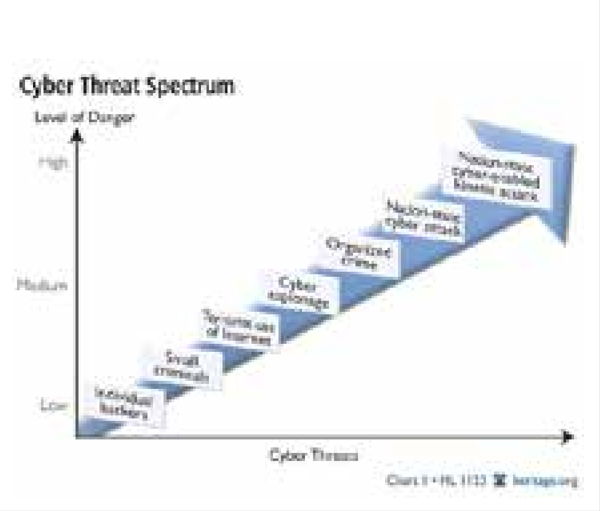


Figure 3: Cyber Threat Spectrum of the various threats and level of danger posed[14]

While connectivity has been advantageous for us, it is this same connectivity in which much vulnerability has spewed from. Such vulnerabilities have resulted from weaknesses in technology as well as improper implementation and oversight of technological products.

Amidst the confusion amongst the many catchwords associated with cyber space, what is cyber power? In this essay, I will subscribe to Daniel Kuehl's definition that cyber power is, "the ability to use cyber space to create advantages and influence events in all the operational environments and across the instruments of power" and is used for achieving the policy objectives of the perpetrator which could be an individual, organisation or nation.[15] Cyber power is therefore premised on the creation, control and communication of digital information via the internet and other digital means. Information is the key element in cyber power and it forms a dimension of the Information instrument of power under the 'Diplomacy, Information, Military and Economic (DIME)' model. With the increased wielding of cyber power militarily, we now bear witness to it becoming part of the military instrument of power too.

While cyber power is commonly used to pursue desired outcomes within cyber space, cyber means could also be employed to pursue desired outcomes outside the cyber space domain.[16] As mentioned, the US DoD has designated cyber space an 'operational domain' to train and defend as they do in the other four operational domains to support national security interests.[17] In comparison with these four operational domains, there is one subtlety that makes cyber space a problematic domain. It is the first man-made domain which has continuously evolved since its creation.

An observer has remarked that versus oceans and mountains that are difficult to move, cyber space can mutate and be switched on or off.[18] While cyber space has no regard to physical geography, it is intrinsically connected and cyber power can generate effects in all the other four operational domains. It is because of this very interconnectivity that cyber space has become, as Clausewitz said regarding a Centre of Gravity (CoG) as, "the hub of all power and movement of which everything depends."[19]

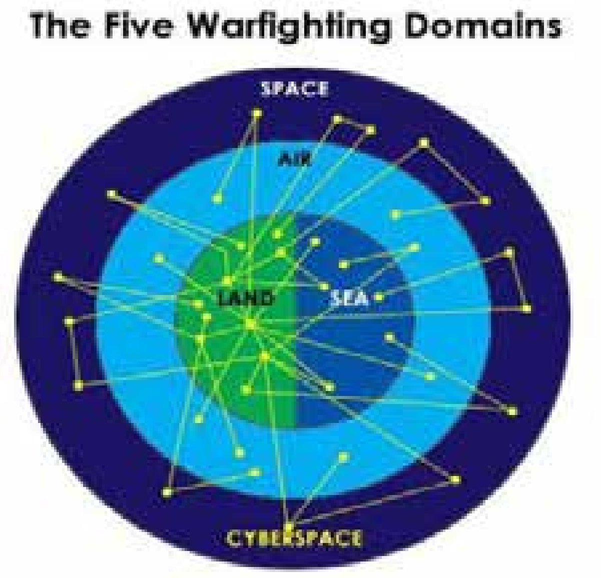


Figure 4: Cyber space – The fifth Operational Domain[20]

DEFINING PERPETUAL DISRUPTION THROUGH CYBER POWER

While hacking and virus-writing began as hobbyist activity not meant to cause serious long-term harm, cyber threats have evolved towards achieving financial and political objectives and have become disruptive and destructive in nature.[21] So, why do individuals, nations or organisations opt to use cyber power? Although cyber attacks are unlikely to be the direct cause of casualties, they can still function as effective tools for political coercion. Strategically, cyber attacks can be employed as an effective coercive weapon to disrupt networks in major financial hubs or to incapacitate critical physical infrastructures (eg. power grids). Tactically, cyber attacks could be used as a brute force weapon to disable or disrupt the internet-connected unclassified military and civilian networks upon which major powers rely to project conventional military force.[22]

Strategically, such attacks cause communications paralysis and hamper the communication of the elites between themselves and with the outside world as well as stifle their reaction to events in a timely manner.

This is similar to what has been famously coined by United States (US) Secretary of Defence Leon Panetta as a 'Cyber Pearl Harbour' to represent a scenario in which adversaries launch attacks on critical infrastructure so as to disable or degrade critical military systems and communication networks.[23] Thus, I would define perpetual disruption through cyber power as never-ending disruption perpetrated by cyber power. The disruption caused would include the following effects defined by the US DoD: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.[24]

EXAMPLES OF CYBER THREATS

With the earlier backdrop of why cyber power is used to perpetrate attacks in cyber space, I will next highlight examples of cyber threats along the Cyber Threat Spectrum that could have been employed by nations or organisations to achieve their policy objectives. These examples illustrate that the effects of cyber attacks are wide spanning, the cyber attacks are highly accessible and the medium of cyber domain is 'boundary-less', thus increasing their attractiveness for the pursuit of political objectives.

Cyber-Terrorism – Attacks Amidst Estonia and Russia Disagreement (2007)

This was the wake-up call to cyber power because it was the first case against an entire nation state. Known as 'Web War 1', a continuous three-week wave of cyber attacks was made on Estonia in April 2007 and swamped websites of Estonian organisations, including government agencies, banks and news agencies.[25] These were Distributed Denial of Service (DDoS) attacks wherein targeted internet sites are flooded by thousands of concurrent visits which overload the bandwidth of the sites' servers. It has been postulated by the Estonians that this crisis was precipitated by Estonia's disagreement with Russia due to plans to relocate the Bronze Soldier of Tallinn memorial. The North Atlantic Treaty Organisation (NATO) responded by sending some of its best cyber terrorism experts to perform investigations and to bolster the Estonian electronic defences. Even though Estonia is one of the most digitally connected states in Europe, the Estonia defence minister conceded that the difficulty in verifying the source of the attacks made it an uphill task and he acknowledged the presence of more safe refuge in cyber space than in the space domain.[26] NATO has since established a 'centre of excellence' for cyber-defence in Estonia to combat such cyber threats.[27] Strategically, such attacks cause communications paralysis and hamper the communication of the elites between themselves and with the outside world as well as stifle their reaction to events in a timely manner.[28]

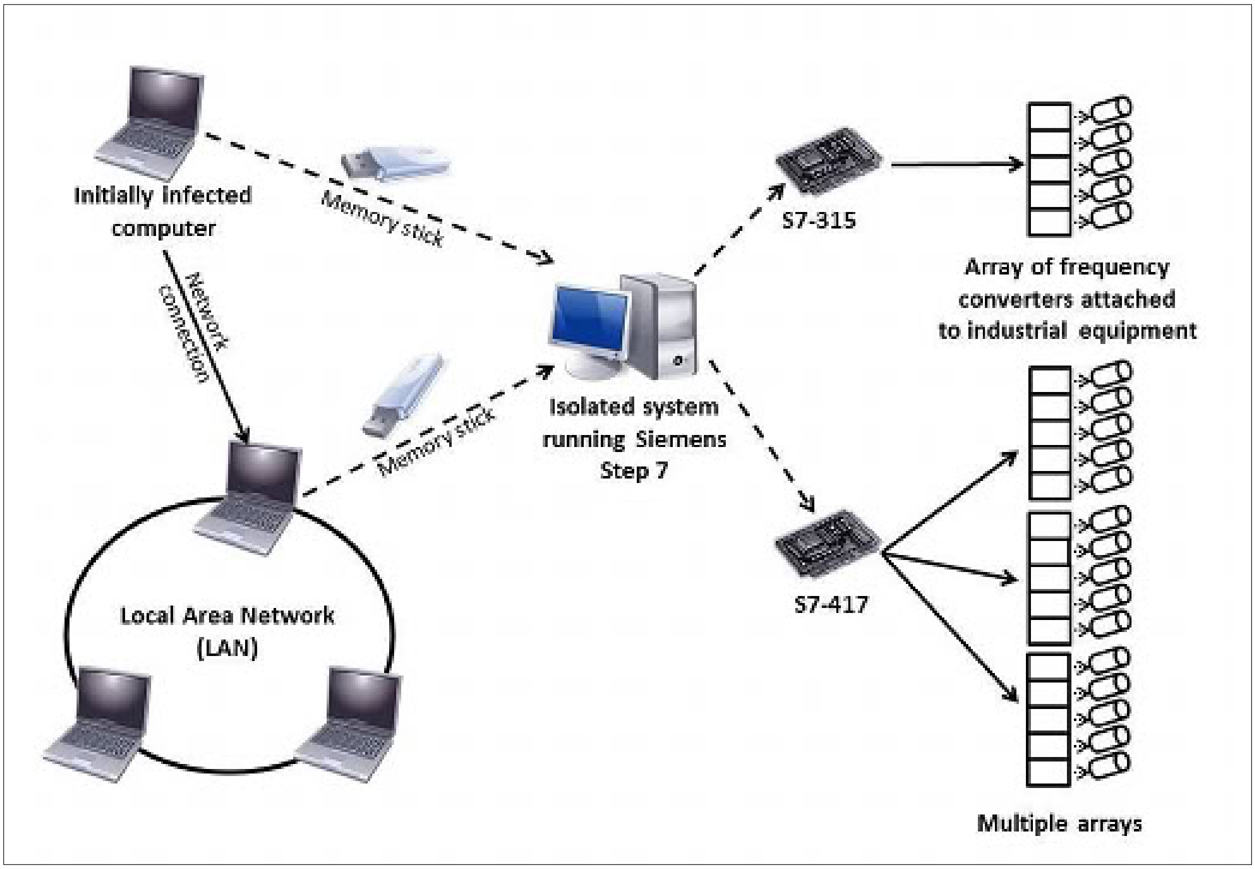

Initially infected computer
Memory stick
Network connection
Memory stick
Isolated system running Siemens Step 7
S7-315
S7-417
Array of frequency converters attached to industrial equipment
Local Area Network (LAN)
Multiple arrays

Figure 5: Propagation of the Stuxnet worm[29]

Cyber-Enabled Kinetic Attack – Delay In Iranian Nuclear Programme (2010)

In 2010, the Stuxnet computer worm infected the Iranian nuclear programme systems and apparently delayed the programme by as much as two years. Respected experts in the computer security field reflected that the Stuxnet attacks were unparalleled and one that nobody hoped to witness again. The worm was designed to attack industrial Programmable Logic Controllers and it sabotaged the control systems that powered the plant's centrifuges.[30] Authorship of the worm remains unknown. The attack is highly significant, as it burst existing security assumptions by damaging industrial systems that were outside the internet and was able to accomplish what five years of United Nations (UN) Security Resolutions could not.[31] The Stuxnet were reported as efforts by America and Israeli to undermine the Iranian pursuit of a nuclear bomb after unnamed officials linked with the programme leaked the story.[32] It is reported that unlike DDoS attacks that could take a few days or weeks to clear up, Stuxnet-like attacks can potentially set back their victims by many years.[33] Strategically, such attacks could be carried out as 'special operations' against an enemy's vulnerabilities and cause disruption by attacking his CoG such as cyber-infrastructure and networks.

Cyber-Espionage – Sham Facebook Account Of Nato Commander (2011)

In 2011, British government officials, Defence Ministry officials and senior military officers were deceived into befriending someone impersonating as US Navy Admiral James Stavridis in Facebook.[34] This allowed their information to be compromised. Even though the fake Facebook account was deleted within 28 hours of being exposed, it was difficult to trace the creator of the account. A NATO spokesperson acknowledged that this was not the first occurrence of someone impersonating an allied commander in the internet. A Federal Bureau of Investigation (FBI) executive assistant director correspondingly admitted that the FBI has witnessed thousands of breaches monthly due to inherent vulnerabilities in infrastructure. He further proclaimed that the FBI knew the capabilities possessed by the foreign states as well as the information that they were targeting. Strategically, such sham attempts to illicitly obtain sensitive information and falsify messages from persons in positions of command and authority, mislead, confuse as well as create mistrust within organisations.[35]

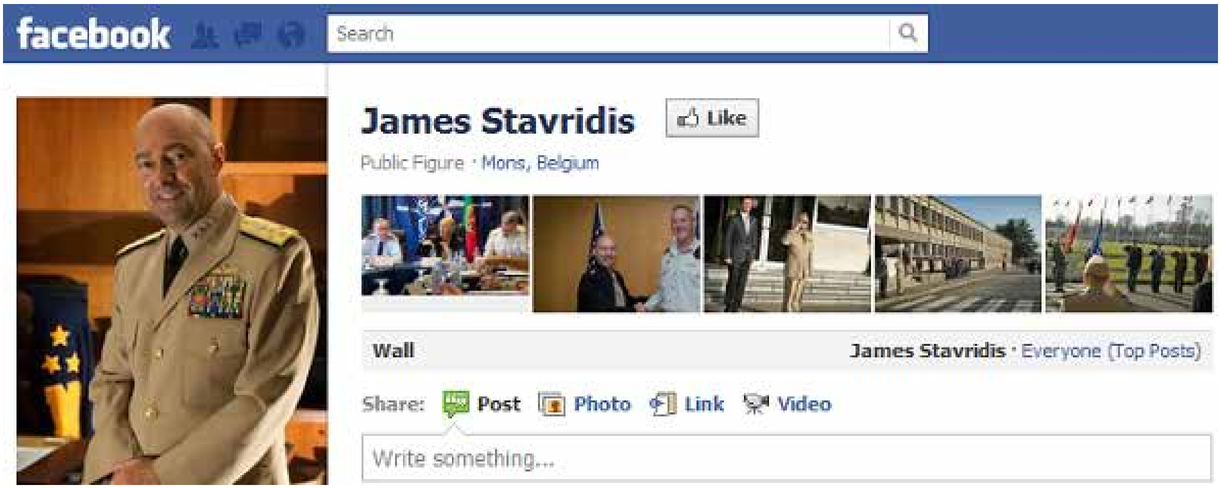


Figure 6: Actual profile of US Admiral James Stavridis.

Cyber Attack – Ukraine And Russia Cyber Conflict (2014)

The on-going hostilities between Ukraine and Russia are mirrored by a corresponding cyber war between the two countries, as evidenced by an analysis of internet traffic. In one instance, a total of 22 Ukrainian computer networks were reportedly infected by the sophisticated 'Snake' virus.[36] They included computer networks that were run by the Kiev government. The number of cyber attacks traded between them appeared to have risen sharply in parallel with worsening relations due to the overthrow of the Yanukovych government and the annexation of Crimea. The cyber attacks were persecuted by a combination of state forces, criminal organisations as well as independent 'patriotic hackers'. Activists and experts have suggested that this is a trend that is likely to recur in future conflicts.[37] Greg Day, vice-president at FireEye, Inc had mentioned that the spread of information technology had expanded the boundaries for conflict and meant combatants no longer had to be armed for conflict.[38] Strategically, these attacks aim to take down the networks and infrastructure of the opponent without the need to employ a military response.

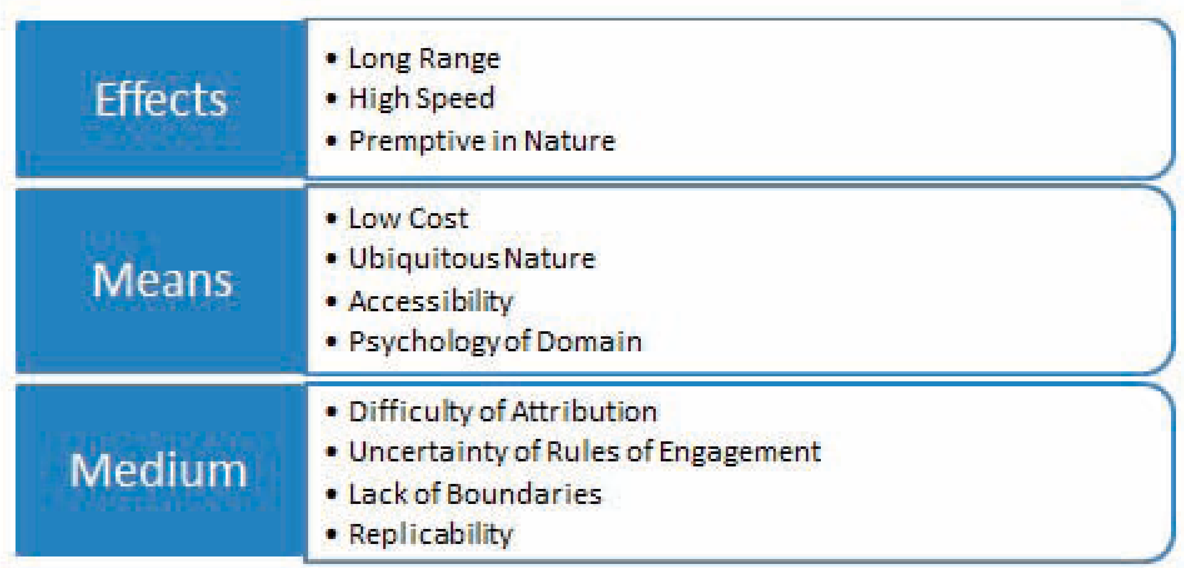
WHY PERPETUAL DISRUPTION?

Based upon the earlier examples, it can be seen that cyber threats can indeed be a means to aid nations or organisations in achieving their policy objectives. But, will cyber power herald an age of perpetual disruption? I posit that it will, based upon the following factors that I will elaborate on, grouped into the following aspects of 'Effects', 'Means' and 'Medium'. I will define 'Effects' as the result of cyberattacks, 'Means' as the instruments of cyber power and 'Medium' as the cyber domain environment.

EFFECTS

Long Range and High Speed

Attacks in cyber space occur at high speeds and seem almost instantaneous to human observers. They subject defences to immense pressure, as the perpetrator has only to be successful once, whereas the defender has to be successful all of the time.[39]



Effects
- Long Range
- High Speed
- Premptive in Nature

Means
- Low Cost
- Ubiquitous Nature
- Accessibility
- Psychology of Domain

Medium
- Difficulty of Attribution
- Uncertainty of Rules of Engagement
- Lack of Boundaries
- Replicability

Figure 7: Factors resulting in Perpetual Disruption by cyber power

Unlike the other four domains, range is not an issue in cyber space and the geographical distance between the attacker and his target is basically immaterial. Attackers can literally target anywhere in the world, regardless of geographical separation.[40] In contrast to the old serial form of war, this parallel process of war actualises what Clausewitz termed the ideal form of war: the "striking of blows everywhere at the same time".[41] Thus, it would appear seemingly unattainable and resource draining to totally defend against all cyber threats and it is rightly pointed out by Frederick the Great that, "he who defends everything defends nothing."[42]

Pre-Emptive In Nature

Typically, cyberattacks are pre-emptive in nature and not detected till the effects are unleashed. Malicious software can be embedded in an adversary's network and lie dormant till it is triggered and causes the intended damage. Cyber attacks will typically favour offence, thus in a crisis situation in which defence is difficult or impossible, leaders on both sides may feel pressured to attack before being attacked, lest their non-cyber forces be rendered ineffective by the adversary's first strike. A surprise cyber strike similar to a 'Cyber Pearl Harbour' could disrupt or disable an adversary's military networks and be followed by a conventional attack that permanently takes out the adversary's physical weapons and/or networks before it is able to bring them back online.[43] Even for exploits that seemingly require fewer resources, like the campaign against Estonia, it is evident that the advantage lies with those who take the offensive.[44]

MEANS

Low Cost

Typically, cyberattacks are pre-emptive in nature and not detected till the effects are unleashed. Malicious software can be embedded in an adversary's network and lie dormant till it is triggered and causes the intended damage.

The cost of entry into the cyber domain is considerably low. Both the expertise and resources required to exploit the cyber domain are modest as compared to the other four domains. Due to its low cost, many argue that it could level the strategic playing field among nations. The former commander of Air Force Cyber space Command, General William Lord had admitted that a laptop computer and an internet connection was all that was required.[45] Colonel Stephen Korns of the United States Air Force (USAF) Joint Task Force has also pointed out that many cyber weapons are now widely available and priced affordably, such as denial-of-service software that could be purchased off the internet and subsequently launched upon the intended target.[46] In fact, this is clearly shown by the cyber attacks against Estonia and Georgia in which the majority of perpetrators, while not programming experts, had downloaded easily available software to carry out their attacks.[47] Furthermore, such attacks may allow the projection of force by the aggressor state without the need to subject its conventional forces to the perils of combat and thereby reducing the anticipated costs of the attack.[48]

Ubiquitous Nature

Cyber space is critical in the everyday functioning of not just the industrially-developed nations, but also the emerging and developing ones. This overwhelming reliance on cyber space throughout the modern society presents an attacker with an abundance of targets, thereby resulting in immense pressure on its successful defence. Cyber power is thus ubiquitous, as it can enable the projection of air, land, sea, and space power as well as influence the four instruments of power represented in the DIME model. Our reliance on cyber space is ever increasing and it would be an easy means for the use of cyber power to potentially do damage to critical infrastructure.

Accessibility

Cyber attacks need not be carried out by states; in fact, the difficulty for non-attribution makes cyberattacks attractive as non-state actors could be the pawns for the state in carrying out the attacks. The proliferation of cyber technologies has ensured that non-state actors as well as individuals with personal vendettas can increasingly exploit asymmetrical means to their advantages vis-à-vis governments.[49] Correspondingly, states could also partake in strategic 'cyber-framing' by launching attacks through proxies such as non-state actors.[50] Cyber attacks can also be favoured by terrorists as the weapons are relatively easy to acquire. The attribution problem would also make them particularly attractive to terrorists, who are often not only risk-acceptant but also may not have a 'mailing address' or infrastructure against which their target could eventually launch a retaliatory strike. Furthermore, many of the cyber attacks have shown that terrestrial distance is immaterial and much of the developed world's critical civilian infrastructure is relatively vulnerable.[51]

Psychology Of Domain

The domain of cyber space is a domain in which would-be penetrators may psychologically feel uninhibited as there is largely no backlash of physical effects or trauma. From the results of the Walter Reed Army Institute of Research (WRAIR) study conducted on the psychological impact of combat duty on soldiers, 10 facts were amalgamated in a brochure to show how the sudden, intense and life threatening nature of combat could psychologically affect soldiers.[52] The unpleasantries of combat represented in the brochure could potentially skew the balance of favour towards non-kinetic conflicts.

MEDIUM

Difficulty Of Attribution

The draw of cyber power for many users is the opportunity to covertly exploit it on a global level without it being attributed to the culprit. As identities are easily masked in cyber space, there is a challenge to attribute attacks to the perpetrators. Even if that is possible, there is added difficulty in determining if he is a representative of a state, a state sponsored actor, a terrorist or just a prankster. As governments cannot be easily made liable for cyber attacks done by private hackers working individually, retaliation becomes an unlikely scenario. Consequently, there is a real danger of misidentifying an attacker, thus harming innocent individuals or targeting the wrong place.[53] As such, databases can be probed for classified or proprietary data, and their owners may be totally oblivious that their information is being compromised. In addition to the innate complexities to attribute the identity and uncover the motivation of attackers, the ability to surreptitiously exploit cyber power makes it particularly attractive to governments and other actors.[54]

Uncertainty Of Rules Of Engagement

The rules of engagement of conventional warfare are clearly enshrined by the Geneva Convention and Article 51 of the UN Charter. However, these rules do not apply in cyber space which is boundless and borderless.[55] While the Pentagon has warned potential adversaries of the consequence of carrying cyber attacks against the US, there are uncertainties on what kind of cyber attacks would constitute a use of force.[56] There is currently no consensus on how regulations would be used to govern cyber conflicts as well as the thresholds for when a disrupting cyber attack becomes a casus belli for a more traditional military response.[57] Furthermore, there is no effective international arrangement that performs law enforcement in cyber space. Given the international nature of many cyber threats, national enforcement efforts will be less effective than an integrated international effort.

Lack Of Boundaries

Cyber space has no boundaries which would mean that national boundaries are not a sufficient deterrence as perpetrators can conduct attacks from anywhere as long as they have access to the internet. This increased interconnectedness in the world as well as the speed of proliferation of new technological products offers more opportunities for cyber attacks. Furthermore, the internet introduces an 'information frontier' which does not possess boundaries within it to demarcate the information borders of individual states from one another. This gives rise to difficulties for states to act on cyber threats due to the lack of territorial boundaries in cyber space.[58] Furthermore, the characteristic of cyber space allows multiple actors to operate in the domain simultaneously from different locations and potentially generate strategic effects that are exponential to that of the other four domains.

Replicability

Cyber space is replicable and can exist in multiple locations at once. Compared to the physical realm which is destructible, cyber space is man-made and is reparable. Every network can hold its own cyber space which therefore results in a limitless number of quasi-independent spaces.[59]

AN AGE OF PERPETUAL DISRUPTION

It is noteworthy that while the frequency of cyber threats is likely to increase, its net effects still remain relatively small and ineffectual as a standalone weapon. However, as there are currently no global norms of behaviour in cyber space, and because it is so attractive and cheap to use, smaller countries or non-state actors can use it to asymmetrically balance larger states' power. In fact, even larger states can use it against smaller states as a proxy to war, to exert coercive influence. Cyber attacks can therefore only

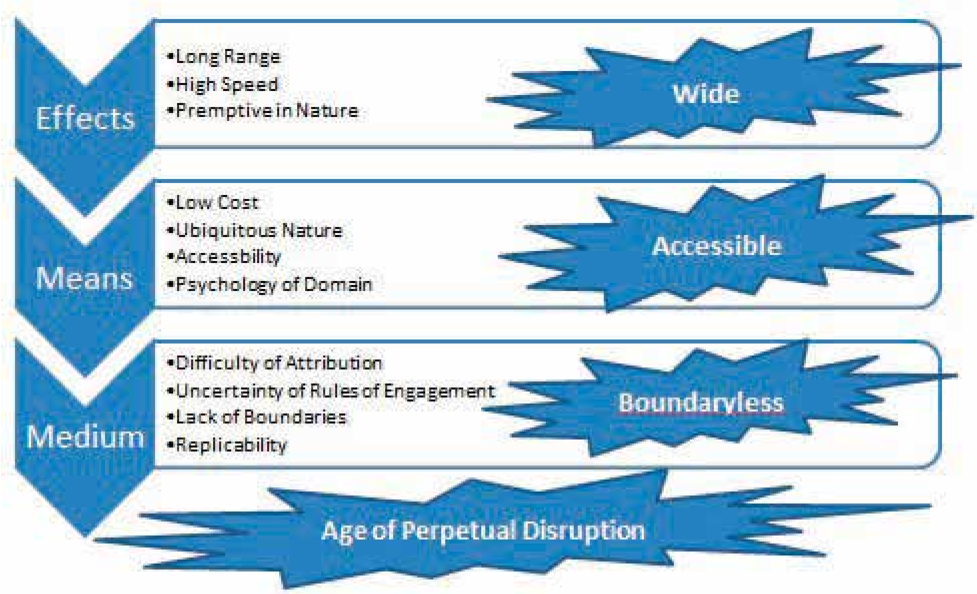


Figure 8: Factors culminating into Perpetual Disruption

become increasingly attractive and prevalent. Thus, based on the aforementioned arguments presented in the areas of 'Effects', 'Means' and 'Medium', I surmise that cyber threats have become the norm and will herald in an age of perpetual disruption as they are wide spanning, accessible and 'boundary-less' as depicted in *Figure 8*.

CONCLUSION

This essay has explored the claims that the rise of cyber power will herald the arrival of an age of perpetual disruption. Through studying the various cyber threats that have occurred, we can see cyber power exploited to achieve the policy objectives of individuals, nations or organisations. I have shown through the factors cited in the areas of 'Effects', 'Means' and 'Medium' that cyber power will indeed herald the arrival of an age of perpetual disruption. However, while the frequency of cyber threats is likely to increase, its net effects still seem small and ineffectual as a standalone weapon. Even if cyber threats are unlikely to reach the effects felt by conventional means, a threat is a threat nonetheless, and we have fortunately not seen them become a casus belli for a military response yet. Nevertheless, with the age of disruption that is dawning upon us, there is a need to take a defence in depth approach so as to provide an overall resilience against the use of cyber power.

ENDNOTES

1. US Department of Defence, "Department of Defence Strategy for Operating in Cyberspace," 2011.
2. Internet World Stats, Internet Growth Statistics, http://www.internetworldstats.com/emarketing.htm.
3. James Adams, *The next World War* (New York: Simon and Schuster, 1998), 93.
4. David Alexander, "Pentagon to treat cyberspace as "operational domain," Reuters, 2011, http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.
5. International Telecommunication Union, "Statistics," 2011, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
6. John B. Sheldon, "The Rise of Cyberpower," in Strategy in the Contemporary World, eds. John Baylis, James J.Wirtz and Colin S.Gray, (*Oxford: Oxford University Press*, 2013), 311.
7. Thomas Jones, "William Gibson: beyond cyberspace," (*The Guardian*, 2011), http://www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace.
8. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Cyber power and National Security, eds. Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, (*Washington, D.C.: National Defence UP*, 2009).
9. Martin Libicki, "Cyberpower and Strategy," Global Strategic Review 2010 Sixth Plenary Session, RAND Corporation, 2010. http://www.iiss.org/en/events/gsr/sections/global-strategic-review-2010-946c/sixth-plenary-session-6e03/martin-libicki-03c2.
10. The White House, "The National Security to secure Cyberspace", 2003.
11. Mary Johnston, "High Density Power Requirement – Can Your Data Centre Support It?" http://www.datasitecolo.com/wp-content/uploads/2014/12/IoT-Graphic.png.
12. Martin Libicki, Conquest in Cyber space – National Security and Information Warfare (*Cambridge University Press*, 2007).
13. This essay will not be considering Cybercrime or Cyberattacks that are persecuted without any policy objectives and for personal gains.
14. T O'Connor, "The Cyberterrorism Threat Spectrum, "http://www.drtomoconnor.com/3400/3400lect06a.htm.
15. Daniel T. Kuehl, "From Cyberspace to Cyber power: Defining the Problem." in Cyberpower and National Security, eds. Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, (*Washington, D.C.: National Defence UP*, 2009).
16. Joseph S. Nye Jr, *Cyber Power.* (Cambridge, Belfer Center for Science and International Affairs, May 2011).
17. U.S. Department of Defence, "Department of Defence Strategy for Operating in Cyberspace," 2011.

18. Gregory J. Rattray, “An Environmental Approach to Understanding Cyberpower,” in Cyber power and National Security, eds. Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, (Washington, D.C.: National Defence UP, 2009), 256.

19. Carl von Clausewitz, *On War,* (*Princeton University Press*, 1976). Edited and translated by Michael Howard and Peter Paret.

20. Tyler Thia, “Country-to-country cyberattacks deemed OK by users,” ZDNet Asia News, 11 Aug 2011, http://www.zdnetasia.com/country-to-country-cyberattacks-deemed-ok-by-users-62202005.htm.

21. Source: Chainsoff's Blog, “Panetta is critical on the security level for NATO networks,” https://i2.wp.com/securityaffairs.co/wordpress/wp-content/uploads/2013/01/warfareDomains.jpg.

22. Liff, Adam P “Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyber warfare Capabilities and Interstate War,” *Journal of Strategic Studies* v._ 35 n._ 3 (2012): 401-428

23. Leon E. Panetta, “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City,” Department of Defence News Transcript, 2011. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

24. US Department of Defence, “Department of Defence Strategy for Operating in Cyberspace,”

25. The Economist, “*War in the fifth domain*,” 2010, http://www.economist.com/node/16478792.

26. Alan Chong, “Information Warfare? The Case for an Asian Perspective on Information Operations.” *Armed Forces & Society*, 2013; 40(4) (2014): 599-624.

27. The Economist, “War in the fifth domain.”

28. Stephen W. Korns and Joshua E. Kastenberg, “Georgia’s Cyber Left Hook,” Parameters, Winter 2008-2009, v._38, n._ 4 (2008): 60.

29. Paulo Shakarian, “Stuxnet: Cyberwar Revolution in Military Affairs,” Small Wars Journal, 2011, http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf.

    Daniel Dombey, “US says cyberworm aided effort against Iran,” (*The Financial Times*, 2010).

30. Ibid.

31. Klaus-Gerd Giesen, “*Justice in Cyberwar*,” Florianópolis, v._13, n._1, (2014): 27-49, http://dx.doi.org/10.5007/1677-2954.2014v13n1p27.

32. David E.Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” (*The New York Times*, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

33. Peter Bright, “Stuxnet apparently as effective as a military strike,” ARS Technica, 2010, http://arstechnica.com/tech-policy/news/2010/12/stuxnet-apparently-as-effective-as-a-military-strike.ars.

34. Emil Protalinski, “Chinese spies used fake Facebook profile to friend NATO officials,” ZDNet, 11 Mar 2012, http://www.zdnet.com/blog/facebook/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials/10389?tag=content;siu-container.

35. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O’Reilly, 2010), 146–50.

36. Tony Morbin, “Russia suspected of Ukraine cyber attack,” SC Magazine, 2010, http://www.scmagazineuk.com/russia-suspected-of-ukraine-cyber-attack/article/337578/.

37. Ben Farmer, “Ukraine cyber war escalates alongside violence,” (*The Telegraph*, 2014), http://www.telegraph.co.uk/news/worldnews/europe/ukraine/10860920/Ukraine-cyber-war-escalates-alongside-violence.html.

38. FireEye, Inc is a publicly listed enterprise cyber security company that provides products and services to protect against advanced cyber threats, such as advanced persistent threats and spear phishing

39. John B. Sheldon, “Deciphering Cyberpower – Strategic Purpose in Peace and War,” Strategic Studies Quarterly, Summer 2011 (2011).

40. Liff, Adam P, “Cyberwar: A New “Absolute Weapon”? The Proliferation Of Cyberwarfare Capabilities And Interstate War.”

41. Warden III, John A, “The enemy as a system,” Airpower Journal; Spring 95, v._9 n._1, (1995): 40.

42. Brainy Quotes, "Fredrick the Great," http://www.brainyquote.com/quotes/quotes/f/frederickt140989.html

43. Liff, Adam P, "Cyberwar: A New "Absolute Weapon"? The Proliferation Of Cyberwarfare Capabilities And Interstate War."

44. John Arquilla, "Cyberwar Is Already Upon Us," Foreign Policy, 2012, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/

45. Glenn Derene, 'The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back', Popularmechanics.com, 2009, http://www.popularmechanics.com/technology/military/42774634.

46. Col Stephen W. Korns, USAF, "Cyber Operations: The New Balance," Joint Force Quarterly v._54, n._3 (2009): 97–98.

47. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do about it (New York: Ecco*, 2010), 11-21.

48. Liff, Adam P "Cyberwar: A New "Absolute Weapon"? The Proliferation Of Cyberwarfare Capabilities And Interstate War."

49. Joseph S. Nye Jr, Cyber Power.

50. Liff, Adam P "Cyberwar: A New "Absolute Weapon"? The Proliferation Of Cyberwarfare Capabilities And Interstate War."

51. Ibid.

52. Walter Reed Army Institute of Research, "10 Tough Facts about Combat Brochure," U.S. Army Medical Research and Materiel Command, http://veteransinfo.tripod.com/battlemindtrainingg.pdf.

53. Dimitar Kostadinov, "The Attribution Problem in Cyber Attacks," Infosec Institute, http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.

54. John B. Sheldon, "Deciphering Cyberpower – Strategic Purpose in Peace and War," Strategic Studies Quarterly, (2011).

55. Army Technology, Elisabeth Fischer, "Cyber Warfare – Do We Need a New Geneva Convention?" 2011, http://www.army-technology.com/features/feature115500/.

56. Siobhan Gorman and Julian E. Barnes, "Cyber Combat : Act of War," The Wall Street Journal, 2011, http://www.wsj.com/articles/SB100014240527023045631045763556231357827 18.

57. John B. Sheldon, "Stuxnet and Cyberpower in War," World Politics Review, 19 Apr 2011, http://www.worldpoliticsreview.com/articles/print/8570.

58. Michael T. Zimmer, "The tensions of securing cyberspace: the internet, state power & the National Strategy to Secure Cyberspace," First Monday, Volume 9, Number 3 (2004).

59. Martin Libicki, *Conquest in Cyber space – National Security and Information Warfare*.

ME5 Calvin Seah Ser Thong is currently a section head in HQ Maintenance and Engineering Support. ME5 Seah holds a Bachelors of Engineering in Mechanical & Production Engineering from the Nanyang Technological University (NTU), Masters of Science in Industrial and Systems Engineering from the National University of Singapore (NUS) and Masters of Science in Defence Technology and Systems from NUS, obtained under the SAF Postgraduate Award. For this essay, he was awarded a book prize for outstanding essay in the Campaign and War Studies module when he attended the 46th Command and Staff Course in 2015.

ME5 Seah is a Business Excellence Assessor, National Innovation and Quality Circle Assessor as well as an American Society of Quality Judge. He was recently awarded the merit prize for his co-written essay in the 2015/2016 CDF Essay Competition. He was a winner of the 1st prize in the CDF Essay Competition 2013/2014 for his co-written article, "Learning From Mother Nature: Biomimicry for the Next Generation SAF," that was published in the August 2015 issue of the Australian Defence Force (ADF) Journal.

Information Technology Advances: Friend or Foe?

by ME5 Su Juncun

Abstract:

Information Technology (IT) has advanced by leaps and bounds over the past few decades. In this essay, the author examines the implications of the advancement of IT on Singapore and the Singapore Armed Forces (SAF). He begins by tracing the rapid growth of IT, and along with it the evolution of cyber warfare, which has opened up a new battlefield in the realm of cyber space and shown the capability to facilitate psychological operations and perception management. On the other side of the coin, the author contends that IT has presented many new opportunities for the SAF to exploit, especially in the areas of learning and training, safety and administration and raising public awareness via social media platforms. By employing a combination of 'Quality' and 'Quantity' safety nets, the SAF may not only be able to counter the threats of cyber attacks, but also reap the many benefits of the advancements in IT to further enhance its effectiveness in defending the nation.

Keywords: Information Technology; Cyber Attacks; Social Media; Virtual Defence; Knowledge Management

INTRODUCTION

Information Technology and its History

IT is the use of systems to store, retrieve and send information.[1] It has come a long way: from clay tablets to preserve ancient Sumerian beer recipes 4,000 years ago, to the first telegram message tapped out by Samuel Morse from Washington to Baltimore in 1844.[2] Since then, IT has improved tremendously and taken new forms.[3]

The Invention and Global Proliferation of the Internet

By 1950, computers had been invented and in 1969, the first area network was operationalised, connecting several United States (US) universities.[4] It eventually evolved into the Internet — a system of networks that spans the globe today.[5] In 1990, there were around 300,000 Internet users. This number jumped to almost 3 billion in 2014.[6] The invention of computers and the Internet, and their derivatives, have since been regarded as the key IT advances in recent decades.

Jumping on the IT Bandwagon

Singapore jumped on the bandwagon in 1998. Then-Prime Minister, Mr Goh Chok Tong mentioned, "...that in order to stay ahead of competition, Singapore must aim to have a knowledge-based economy."[7] The government recognised that IT would play a crucial role and invested in extensive infrastructure development, e.g. the island-wide broadband.[8] This effort cumulated into the iN2015, a 10-year masterplan in May 2005, which was developed to grow the infocomm sector and technologies further.[9] By 2012, 84% of households had home broadband Internet access.[10]

Impact on National Defence: Susceptibility to Cyber Attacks

The world 'shrank' with IT advances. While this promoted economic growth in many countries, there were other complications. In the area of National Defence, it raises weighty questions about the possibility of Singapore and the Singapore Armed Forces (SAF) becoming more susceptible to cyber attacks.

> *"Technology... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other."*
>
> *-Carrie Snow*[11]

In this essay, the author aims to illustrate the potential adverse effects of cyber warfare on Singapore and the SAF; highlight the areas of opportunity for the SAF; and suggest possible defences against cyber attacks.

THE SNARES OF IT: CYBER WARFARE

Cyber Warfare is not new, but has evolved with IT advances

The importance of the control of information has existed since early history.[12] During the Napoleonic Wars, Emperor Napoleon I was defeated as his strategic sea communications were cut by the British Royal Navy.[13] This compromised the integrity of Napoleon's information environment.[14]

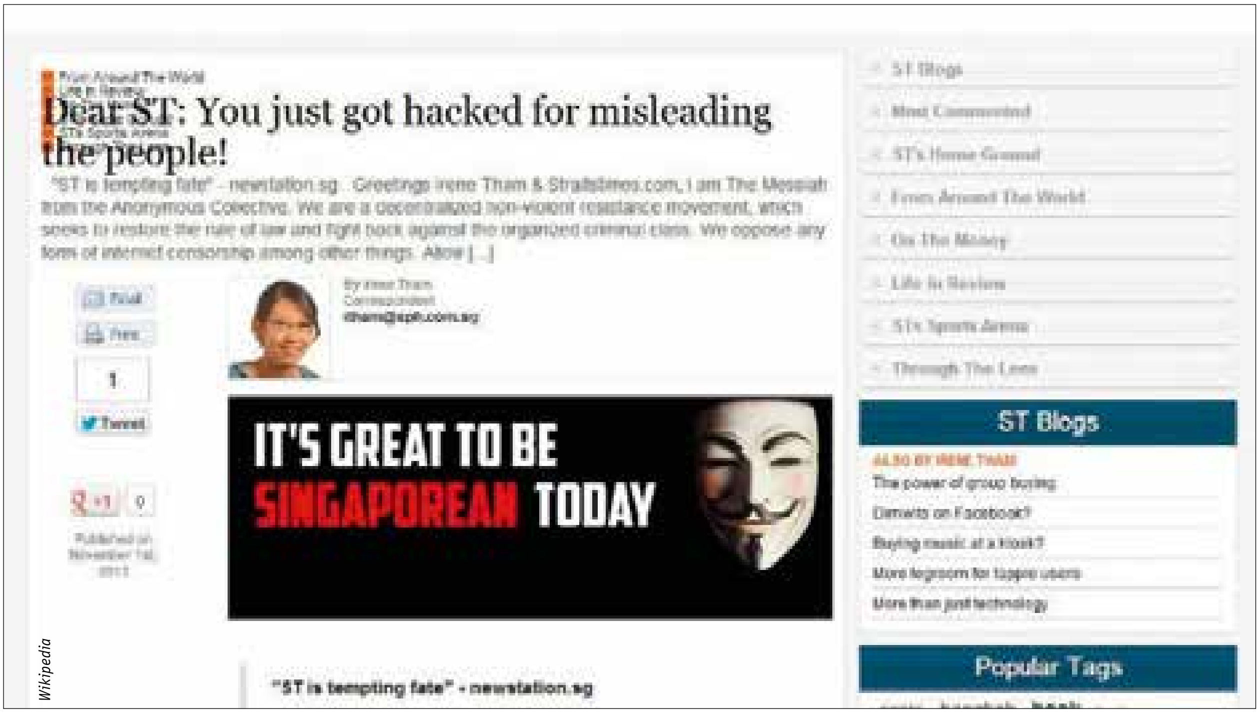
In this modern Information Age, cyber warfare has evolved and has been made potent by the Internet. The Internet is still the fastest communications system invented — it is easily accessible and grants users the protection of anonymity.[15] Therefore, where National Defence is concerned, Singapore and the SAF must not neglect the prowess of modern cyber warfare. The fight to control information will now comprise conventional warfare, cyber war and 'mental war.'[16] Any Singaporean or Singapore Armed Forces (SAF) serviceman may be drawn insidiously into this hybrid battlefield, right at their doorstep through IT.

Cyber war is Real and Implicates Decision-Making Processes

Cyber war, battle in the cyber space, controls information by wreaking havoc on IT systems. Between April 1990 and May 1991, five hackers from the Netherlands penetrated computer systems at American military sites and gained access to information about the US troop locations and weaponry details in the Gulf region.[17] While the hackers' primary objective was the profit from selling this classified information, they could have thwarted the US supplies and potentially altered the outcomes of the Gulf War by sending toothbrushes instead of bullets![18]

In 2007, the first documented case of cyber war intended to cause physical damage took place. A computer worm called Stuxnet was used to retard Iran's nuclear-weapons programmes at Natanz. Stuxnet turned valves on and off and meddled with the centrifuges, wasting uranium and damaging equipment.[19]

These examples illustrate some possibilities from a cyber war, but it could also affect the SAF's warfighting capability in another way. A potential adversary can slow down the SAF's decision-making process which would be instrumental in winning a war.[20] In this Information Age, information and its sources are aplenty and consequently, there are possible 'hackable' opportunities to upset the information that the SAF receives. Without the ability to confirm the veracity of the vast information received, the SAF would end up in a state of decision paralysis, needing to seek confirmation before deciding and acting.[21]



Dear ST: You just got hacked for misleading the people!

"ST is tempting fate" - newstation.sg . Greetings Irene Tham & Straitstimes.com, I am The Messiah from the Anonymous Collective. We are a decentralized non-violent resistance movement, which seeks to restore the rule of law and fight back against the organized criminal class. We oppose any form of internet censorship among other things. Allow [...]

By Irene Tham
Correspondent
itham@sph.com.sg

Published on November 1st, 2013

"ST is tempting fate" - newstation.sg

ALSO BY IRENE THAM
The power of group buying
Dimwits on Facebook?
Buying music at a kiosk?
More legroom for laptop users
More than just technology

Wikipedia

In 2013, online hacktivist group Anonymous launched a wave of cyber attacks on several Singapore-based websites, including The Straits Times.

Psyops and Perception Management

Cyber warfare can also take place in the 'mental space.' Psyops and perception management, which involve toying with the minds and behaviours of individuals, were already employed in the Gulf War where 70% of the Prisoners of War (POWs) reported that their decisions to surrender were influenced by the (psyops) leaflets.[22] A captured general shared that, "Second to the allied bombing campaign, psyop leaflets were the highest threat to the morale of the troops."[23] The Internet provides a convenient means of employing psyops and perception management through constructing a false reality in the cyber space. There exists a risk of an adversary uploading false information into one's databases in an attempt to influence undesirably.[24]

This can affect the SAF and the public as well.[25] As observed by Deputy Prime Minister Teo Chee Hean in 2014, "(We) are all also becoming increasingly dependent on cyber technologies for our daily activities, and the smooth and effective functioning of essential services. The cyber domain has thus become a lucrative target for those who aim to do harm."[26] In 2014 alone, we have seen major security breaches around the world. Globally, Sony Pictures Entertainment suffered from a major online attack while locally, karaoke entertainment operator K Box and Nanyang Polytechnic's databases were hacked.[27] In these cases, sensitive information was obtained and leaked. Therefore, it is not inconceivable that potential adversaries could hack similar computer systems, insert psyops 'e-leaflets' and influence the public and SAF servicemen unfavourably.

The Allure of Cyber Warfare – Affordable and Easily Propagated

Cyber warfare is cheaper and yet can be equally (if not more) potent. A cyber warfare team of 10 to 20 hackers using state-of-the-art computers could potentially accomplish the same objectives as a conventional military force to cause an enemy to surrender.[28] The reality is sobering as modern IT has created new possibilities for offensive cyber warfare to take place in an instant, from anywhere in the world.[29]

The reality is sobering as modern IT has created new possibilities for offensive cyber warfare to take place in an instant, from anywhere in the world.

Against this backdrop, Singapore being rated second in the global Networked Readiness Index (NRI) would be especially vulnerable.[30] The advent of social media such as Facebook, Twitter and Youtube and its widespread usage in Singapore have exacerbated the problem.[31] Furthermore, the modern Information Age has seen the advent of digital devices. From computers to handphones and tablets, these devices allow faster Internet access, at greater convenience. They have created more opportunities for the world to invade and cause collateral damage unbeknown to us, in the form of malicious codes and viruses.[32]

THE SILVER LINING IN THE CLOUD OF IT ADVANCES

The advancement in IT is not just foe and no friend to the SAF. In fact, IT possesses immense potential and presents new opportunities for the SAF in the areas of learning and training, safety and administration and raising public awareness via the social media.

Learning and Training

IT advances present many avenues to enhance operational learning and training in the SAF. In 2009, Basic Military Training (BMT) recruits were issued laptops to access self-directed learning online tutorials before actual hands-on experience. These

Tablet computers are employed in the SAF to enhance operation learning and training.

tutorials covered military fundamentals such as weapons handling and first aid procedures. In 2011, various SAF training institutes turned to the tablets, which made learning even more accessible.[33]

To enhance training realism, the Air Force Training Command has developed two simulators: the Virtual Reality Aircraft Recognition (VRAR) simulator which enables trainees to see aircraft approaches in three dimensions (3D); and the Virtual Hangar Trainer (VHT) which provides 3D virtual reality to train the maintenance crew on aircraft maintenance procedures and emergency response procedures.[34] The VHT also features recording functions and allow trainees to reflect, analyse and learn from their and others' mistakes.[35]

In the Republic of Singapore Navy (RSN), interactive online applications (apps) were built. For example, the 'Visual Signalling – Flashing' and 'Visual Signalling – Flag Hoisting' apps, developed in 2013, enabled naval communications trainees to learn key naval communications methods: transmitting Morse codes via light flashes and sending messages through flag hoisting. The apps allow self-learning, without the need of a dedicated instructor. With these apps, Headquarters Maritime Training and Doctrine Command was able to shorten the learning process and make lessons more effective.[36] Other examples include the US Marine Corps' pilots who use iPads loaded with digital maps. This has helped reduce their workload in the cockpit as they are now able to search for locations without the need to flip through bulky map packs.[37]

Safety and Administration

IT can enhance administrative and safety processes as well. Since 2013, certain administrative processes have been made easier with the launch of the 'MyNSAdmin' and the 'My eLeave and eClaims' apps. SAF Operationally-Ready National Servicemen (NSmen) can utilise the 'MyNSAdmin' app to notify the Ministry of Defence (MINDEF) of their overseas trips without needing to find a computer terminal. In addition, the app will automatically prompt the NSmen to do their overseas notification when they are at the airport or near any immigration checkpoint.[38] Via the 'My eLeave and eClaims' app, Full-Time National Servicemen (NSFs) also gained the flexibility of managing their annual leave plans and submitting transportation, medical and dental claims through their smartphones.[39]

Figure 1: 'My eLeave and eClaims' App[40]

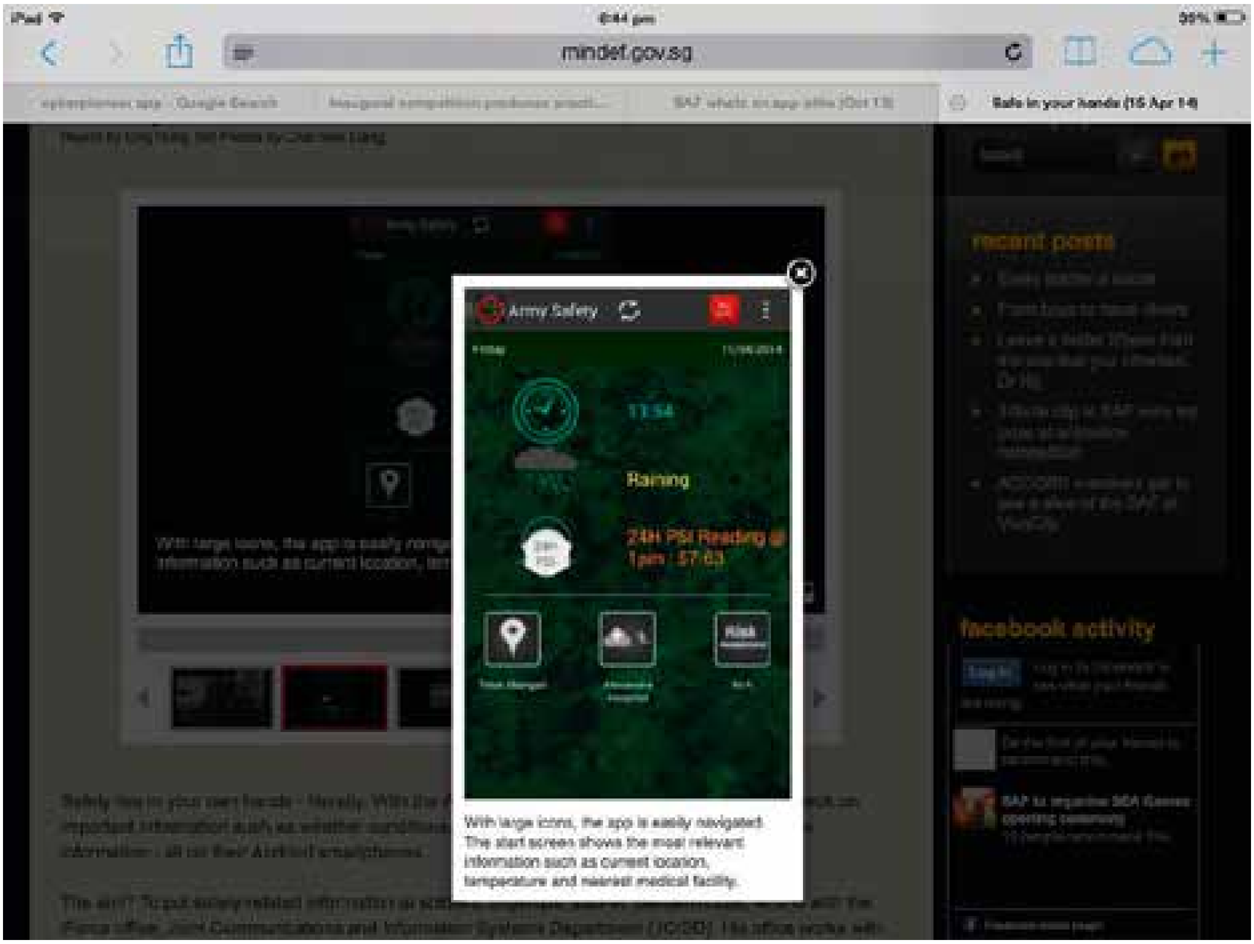
To improve the management of safety, the 'Army Safety' app was launched in April 2014. Through this app, commanders and soldiers can quickly check on vital information such as weather conditions, location of nearby medical facilities and associated route information. "While (the app) does not replace any existing safety measures, it functions as a convenient and complementary source of information," said CPT Muhd Noor Ehsan from the Army Safety Inspectorate (ASI). The app can also be used to report safety hazard reports to the ASI.[41]

Such public outreach not only generates awareness, but also promote positive images of the SAF in general. These have far-fetching effects such as enhancing the public's confidence and support of the SAF. It may even achieve some degree of deterrence effects.

Public Awareness through Social Media

As social media gains traction globally, the SAF has also leveraged on these platforms to create greater awareness and understanding of the SAF. One example is 'The Singapore Army' Facebook page. Managed by the Army Information Centre, this page shares stories, features, photos and videos about the Army. Interestingly, the page also features a summary of its history and key milestones since 1957.

When the Youtube series, 'Every Singaporean Son' first aired in 2010, it created much interest among the public, for this was the first time the SAF BMT in Pulau Tekong had been filmed and broadcasted. Said Mr. Donald Chew, Head of Defence Information



mindef.gov.sg

Safe in your hands (15 Apr 14)

Army Safety

Raining

24H PSI Reading @ 1pm : 57-63

With large icons, the app is easily navigated. The start screen shows the most relevant information such as current location, temperature and nearest medical facility.

recent posts

facebook activity

Figure 2: 'Army Safety' App[42]

Television, "We hope to get people to understand more about BMT."[43] Such public outreach not only generates awareness, but also promote positive images of the SAF in general. These have far-fetching effects such as enhancing the public's confidence and support of the SAF. It may even achieve some degree of deterrence effects.

SAFETY NETS

Virtual Defence

As Singapore becomes more networked and as the SAF continue to invest in more interoperable and networked infrastructure and systems, the relevance of virtual defence becomes more evident. This can also be seen in the US where the main threat to its Internet security is the sheer size of its Internet presence.[44] It will be increasingly difficult to keep out cyber warfare-capable adversaries. Nevertheless, resilient virtual defence can be and have been built to counter such threats. For instance, the US Department of Defense (DoD) employs strategies of both 'quantity' and 'quality' in building its Internet defences, by creating layers of defences with superior security software.[45] These form the backbone to the proposed virtual defence presented in the section below.

(I) Checks and Balances ('Quality' Strategy)

The IT workflows can be enhanced through appropriate policing and monitoring. Policing helps prevent information from being abused in a way that goes against the interests of security. This could be done by incorporating monitoring mechanisms that will provide the necessary checks and balances. Separately, there must also be safeguards against over-reliance on Artificial Intelligence, having machines talking to machines without a human supervising the conversation. Systems need to leave an aperture for control by humans to avoid the problems of passive neglect or runaway processing.[46]

(II) Be Ahead of the Game ('Quality' Strategy)

In building the virtual defence, the SAF must seek continuous improvements in order to stay ahead of the game, as the speed at which IT advances has outpaced current IT security solutions. Now, each IT security cycle begins with the use of the latest known effective software, and ends with the perfection of the newest escalation in attack mechanisms. The timeline for this cycle may soon be a matter of only hours.[47] As such, it is imperative that the SAF invests in Research and Development to stay ahead of this IT power curve. Another aspect is to share best practices and learn from other related agencies such as the Singapore Cyber Security Agency.[48]

(III) Be Extensively Armoured ('Quantity' Strategy)

Following the DoD's strategy of 'quantity', the SAF should also not 'put all its eggs in one basket'. In IT security terms, it translates to avoiding a single point of failure. By using a variety of layered virtual defences, information can be given the highest level of protection.

One of the major failure points is the inability to spot espionage or sabotage acts. A 'two-person control' would counter this vulnerability by setting up critical information workflows such that they must be executed by two (or more) persons. Examples include dual signatures or multiple authorisations. The rationale is that someone is less likely to abuse information if another person must be convinced to go along with the act.[49]

Backup systems are another way of preventing failures. Even if information or systems are sabotaged, there is an extra copy available. Any information should be backed up and protected against accident, natural disaster, or sabotage. Establishing reliable backup facilities is one of the main elements of a successful virtual defence system.[50]

(IV) Educated Servicemen ('Quantity' and 'Quality' Strategies)

To employ and execute virtual defence effectively, there must be proficient servicemen. In addition, humans are found to be the major vulnerabilities of IT security breaches. Education is therefore another important tenet to virtual defence. Security awareness and training programmes will serve to inform servicemen about the SAF's IT security policy, to sensitise them to risks and potential losses, and to train them in the use of security practices and technologies.[51]

In the current context of social media proliferation, the educational process should also emphasise the associated risks as well.[52] This, in the long run, will assist the SAF to build a quality IT security-savvy corps comprising of informed individuals who can provide the layered defences, such as the 'two-person' control, as discussed earlier.

Knowledge Management

On top of building a strong virtual defence, countering a cyber warfare battle also involves gaining an information advantage over the adversaries. One of the ways is to strengthen the decision-making process, through quicker, more thorough and better management of information. Effective Knowledge Management (KM) is one key enabler to this and may be associated with the use of a dynamic database, easily accessible applications and communications within an assured bandwidth. The goal is to blend the best intellects and IT available to turn information into knowledge faster than an adversary.[53]

Emergency Response Team

Last but not least, if the defences fail, the SAF must be prepared to react with an emergency response team. A reference would be the Singapore Computer Emergency Response Team (SingCERT), established in 1997 as a one-stop centre for security incident response in Singapore. It facilitates the detection, resolution and prevention of security related incidents on the Internet.[54] Another key service that SingCERT provides is collaborating with the industry, local and other national CERTs to resolve security incidents collectively. Having come a long way, the SingCERT, now known as the Cyber Security Agency since 2015, would be a worthy agency for the SAF to learn from.

CONCLUSION

> *"Good, bad or indifferent, if you are not investing in new technology, you are going to be left behind."*
>
> *–Philip Green*[55]

The advances in IT are unlikely to be reversed. Bearing in mind the inevitable global proliferation of IT, the world will 'shrink' further. The adverse effects of cyber warfare will become even more pertinent and perilous. In this setting, it is imperative that the SAF invests dedicated resources into IT security by building a combination of 'Quality' and 'Quantity' safety nets, managed and executed by informed servicemen. The SAF Cyber Defence Operations Hub, formed in 2013, is a good start as IT security experts are amalgamated under a single entity to counter digital warfare and beef up defences against online threats.[56]

In this setting, it is imperative that the SAF invests dedicated resources into IT security by building a combination of 'Quality' and 'Quantity' safety nets, managed and executed by informed servicemen.

The logical way forward would be to take advantage of the many opportunities afforded by IT advances. The SAF will be able to enhance aspects such as learning and training, safety and administration and also harness other intangible positive outcomes from raising public awareness through the use of social media.

BIBLIOGRAPHY

“Annual Survey on Infocomm Usage in Households and by individuals for 2012,” (*Infocomm Development Authority of Singapore*, 2015), http://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2012/2012HHmgt.pdf.

Berkowitz, Bruce D. *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press, 2003.

Bilbao-Osorio, Beñat, Dutta, Soumitra and Lanvin, Bruno, Editors, “Rewards and Risks of Big Data”, *The Global Information Technology Report 2014*, 2014.

Campen, Alan D. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, Va.: AFCEA International Press, 1996.

Chow, Jermyn, “SAF Sets up New ‘Cyber Army’ to Fight Digital Threats,” (*The Straits Times*, 2013), http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630.

Denning, Dorothy Elizabeth Robling, *Information Warfare and Security*, New York: ACM Press, 1999.

Dunnigan, James F. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press, 2002.

“Every Singaporean Son,” (*MINDEF*, 2010), http://www.mindef.gov.sg/imindef/resourcelibrary/videos/docus/evrySporeanSon.html#.VOsZC_lhuSp.

Fu Wei’en Eugene and Nah Jinping, “Understanding the Millennial Generation: Developing a More Effective Workforce for the Future SAF”, *POINTER*, v._39, n._ 1, 2013.

Hall, Wayne M. *Stray Voltage: War in the Information Age. Annapolis*, Md.: Naval Institute Press, 2003.

“How Cyber War-fare Really Started – and Where it will lead,” (*The Economist*, 2014), http://www.economist.com/news/books-and-arts/21635967-how-cyber-warfare-really-startedand-where-it-will-lead-turning-worm.

“iN2015 Masterplan,” (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/iN2015-Masterplan.

Infocomm Development Authority of Singapore, “Infocomm Usage – Households and Individuals,” 2014, Selected Primary Internet Activities by Age Group (2012) – Communication Activities, http://www.ida.gov.sg/Infocomm-Landscape/Facts-and-Figures/Infocomm-Usage-Households-and-Individuals#7.

“Infocomm Security,” (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/Infocomm-Security.

Kwang, Kevin, “5 Security Threats to Watch Out for in 2015”, (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/technology/5-security-threats-to/1534772.html.

Kwang, Kevin, “Cyber Warfare needs a ‘Geneva Convention’: Israel’s Space Agency Chairman,” (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/singapore/cyber-warfare-needsa/1421010.html.

Lee Hsiang Wei, “Managing the Risks of Social Media in the SAF”, *POINTER*, v._39, n._2, 2013.

Leong Wai Kit, “Seven Cyber Security Projects to get Funding Boost from NRF,” (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/singapore/seven-cybersecurity/1415680.html.

Lieutenant General John L. Woodward, Jr, “Statement of: Lieutenant General John L. Woodward, Jr, USAF Deputy Chief of Staff, Communications and Information United States Air Force on Information Assurance,” (*The Information Warfare Site*, 2001), http://www.iwar.org.uk/cip/resources/ia-hearing-2001-05/01-05-17woodward.htm.

Lur, Xavier, “SAF to arm new recruits with iPADS,” (*Yahoo News*, 2011), https://sg.news.yahoo.com/blogs/fit-to-post-technology/saf-arm-recruits-ipads-093835831.html.

“Nanyang Polytechnic Alumni Database Breached, Bank Details Stolen”, (*Channel News Asia*, 2015), http://www.channelnewsasia.com/news/singapore/nanyang-polytechnic/1648374.html

Ng Wei-Jin, “Overcoming Digital Turbulences for the 3rd Generation RSAF,” (*POINTER*, 2010), http://www.mindef.gov.sg/content/imindef/publications/pointer/journals/2009/v35n1/feature5.html.

Ong Hong Tat, “Safe in Your Hands,” (*MINDEF*, 2014), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/apr/15apr14_news2.html#.VOr-hY0cT4h.

Ong Hong Tat, “Transforming Learning,” (*MINDEF*, 2012), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2012/aug12_fs2.html#.VOsVb40cT4g.

Quinn, Matt and Taylor, Chris, “Managing Big Risks and Rewards of Big Data,” *The Global Information Technology Report 2014*, 2014.

“Social Analytics (SA) for Business Enterprises Call-for-Collaboration (CFC),” (*Infocomm Development Authority of Singapore*, 2013), http://www.ida.gov.sg/Collaboration-and-Initiatives/Collaboration-Opportunities/Store/Social-Analytics-SA-for-Business-Enterprises-Call-for-Collaboration-CFC.

“Statement by 2nd Minister at COS Debate 2007,” (*Infocomm Development Authority of Singapore, 2007*), https://www.ida.gov.sg/About-Us/Newsroom/Speeches/2007/20060822111238.aspx.

Tan Guan Wei, “SAF Whets an App-etite,” (*MINDEF*, 2013), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/oct13_cs.html#.VOr6D_lhuSr.

ENDNOTES

1. “Definition of Information Technology,” (*Oxford University Press*, 2014), http://www.oxforddictionaries.com/definition/english/information-technology.

2. Bruce D. Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century*, New York: Free Press, 2003, 1-2.

3. Ibid.

4. The Advanced Research Project Agency Network (ARPANET). Dorothy Elizabeth Robling Denning, *Internet Besieged: Countering Cyberspace Scofflaws, New York: ACM Press*, 1998, 15-27.

5. Dorothy Elizabeth Robling Denning, I*nternet Besieged: Countering Cyberspace Scofflaws*, New York: ACM Press, 1998, 15-27.

6. Victor Luckerson, “Internet Users Surge to Almost 3 Billion Worldwide,” (*TIME*, 2014), http://time.com/3604911/3-billion-internet-users/.

7. Goh Chok Tong, "S'pore Gears up for New Growth Wave," Address at the Opening Dinner at the World Economic Forum's annual East Asia summit on 13 October 1998, The Straits Times, 1998.

8. Ibid.

9. “iN2015 Masterplan,” (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/iN2015-Masterplan.

10. “Annual Survey on Infocomm Usage in Households and by individuals for 2012,” (*Infocomm Development Authority of Singapore*, 2015), http://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2012/2012HHmgt.pdf.

11. Carrie Snow, “Carrie Snow Quotes,” *Brainyquote*, http://www.brainyquote.com/quotes/quotes/c/carriesnow108049.html.

12. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, New York: Citadel Press, 2002. 104-110.

13. John Arquilla and David Ronfeldt, “Cyberwar Is Coming!” *Comparative Strategy*, v._12, 1993, 141-165.

14. Loyal Rue, *By the Grace of Guille: the Role of Deception in National History and Human Affair*, Oxford University Press, New York, 1994, 120-122.

15. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, New York: Citadel Press, 2002. 104-110.

16. Michael L. Brown, “The Revolution in Military Affairs: The Information Dimension,” in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Campen, Alan D., Fairfax, Va.: AFCEA International Press, 1996, 43.

17. Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, New York: ACM Press, 1999, 3-4.

18. Gina Smith, "Hackers Could Switch Toothbrushes for Bullets," (*ABCNews.com*, 1997).

19 . "How Cyber War-fare Really Started – and Where it will lead," (*The Economist*, 2014), http://www.economist.com/news/books-and-arts/21635967-how-cyber-warfare-really-startedand-where-it-will-lead-turning-worm.

20. Typically takes the form of an OODA (Observe, Orient, Decide and Act) loop.

21. Wayne M. Hall, *Stray Voltage: War in the Information Age, Annapolis*, Md.: Naval Institute Press, 2003, 25.

22. John Petersen, "Information Warfare: The Future," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., *Cyberware: Security, Strategy and Conflict in the Information Age, AFECEA International Press, Fairax*, VA, 1996, 219-226.

Stephen T. Hosmer, *Psychological Effects of US Air Operations in Four Wars 1941 – 1991*, Rand, Santa Monica, CA, 1996, 143-148.

23. Chad R. Lamb, "Military Psychological Operations," term paper for COSC 511, May 4, 1997, citing "US Army Special Forces: The Green Berets – US Special Operations Command: Psychological Operations," http://users.aol.com/armysof1/PSYOPS.html.

24. Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in *Cyberwar: Security, Strategy, and Conflict in the Information Age, Campen*, Alan D., Fairfax, Va.: AFCEA International Press, 1996, 46.

25. John Rendon, "Mass Communication and Its Impact," in National Security in the Information Age, James P. McCarthy ed., Conference Report, US Air Force Academy, February 28-March 1, 1996.

26. Leong Wai Kit, "Seven Cyber Security Projects to get Funding Boost from NRF," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/singapore/seven-cybersecurity/1415680.html.

27. Kevin Kwang, "5 Security Threats to Watch Out for in 2015," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/technology/5-security-threats-to/1534772.html.

"Nanyang Polytechnic Alumni Database Breached, Bank Details Stolen," (*Channel News Asia*, 2015), http://www.channelnewsasia.com/news/singapore/nanyang-polytechnic/1648374.html.

28. Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, New York: ACM Press, 1999, 17.

29. Ibid.

30. Beñat Bilbao-Osorio, Soumitra Dutta and Bruno Lanvin, "Rewards and Risks of Big Data," *The Global Information Technology Report 2014*, 9-15.

31. "Social Analytics (SA) for Business Enterprises Call-for-Collaboration (CFC)," (*Infocomm Development Authority of Singapore*, 2013), http://www.ida.gov.sg/Collaboration-and-Initiatives/Collaboration-Opportunities/Store/Social-Analytics-SA-for-Business-Enterprises-Call-for-Collaboration-CFC.

32 . Symantec's Vice-President of Product Management for Mobility Michael Lin told Channel NewsAsia that mobile malware has risen by about 300 times in the past year. He added that the company's mobile application (app) insight tool, which inspects 15 million apps in 40 per cent of Android app stores, found that about 900,000 apps had malicious code in them. Kevin Kwang, "5 Security Threats to Watch Out for in 2015," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/technology/5-security-threats-to/1534772.html.

Ng Wei-Jin, "Overcoming Digital Turbulences for the 3rd Generation RSAF," (*POINTER*, 2010), http://www.mindef.gov.sg/content/imindef/publications/pointer/journals/2009/v35n1/feature5.html.

33. Xavier Lur, "SAF to arm new recruits with iPADS," (*Yahoo News*, 2011), https://sg.news.yahoo.com/blogs/fit-to-post-technology/saf-arm-recruits-ipads-093835831.html.

34. Ng Woon Teck Ryan, "A Maintenance Simulator for Air Force Engineers: The RSAF Experience," *IAL Adult Learning Symposium 2014*, 2014.

35. Ibid.

36. Tan Guan Wei, "SAF Whets an App-etite," (*MINDEF*, 2013), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/oct13_cs.html#.VOr6D_lhuSr.

37. Xavier Lur, “SAF to arm new recruits with iPADS,” (*Yahoo News*, 2011), https://sg.news.yahoo.com/blogs/fit-to-post-technology/saf-arm-recruits-ipads-093835831.html.

38. Tan Guan Wei, “SAF Whets an App-etite,” (*MINDEF*, 2013), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/oct13_cs.html#.VOr6D_lhuSr.

39. Ibid.

40. Ibid.

41. Ong Hong Tat, “Safe in Your Hands,” (*MINDEF*, 2014), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/apr/15apr14_news2.html#.VOr-hY0cT4h.

42. Ibid.

43. “Every Singaporean Son,” (*MINDEF*, 2010), http://www.mindef.gov.sg/imindef/resourcelibrary/videos/docus/evrySporeanSon.html#.VOsZC_lhuSp.

44. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, New York: Citadel Press, 2002. 253.

45. Ibid.

46. Matt Quinn and Chris Taylor, “Managing Big Risks and Rewards of Big Data,” *The Global Information Technology Report 2014*, 64.

47. Alan D. Campen, *Cyberwar: Security, Strategy, and Conflict in the Information Age, Fairfax*, Va.: AFCEA International Press, 1996, 280.

48. Kevin Kwang, “Cyber Security Agency will spur 'pro-active' security-first mindset among firms: Yaacob”, (*Channel News Asia*, 2015), http://www.channelnewsasia.com/news/business/cyber-security-agency/1678994.html.

49. Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, New York: ACM Press, 1999, 384.

50. Ibid.

51. Ibid., 382.

52. Lee Hsiang Wei, “Managing the Risks of Social Media in the SAF”, *POINTER*, v._39, n._ 2, 2013, 19.

53. Wayne M. Hall, *Stray Voltage: War in the Information Age, Annapolis*, Md.: Naval Institute Press, 2003, 132.

54. “Infocomm Security,” (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/Infocomm-Security.

55. Philip Green, “Philip Green Quotes,” *Brainyquote*, http://www.brainyquote.com/quotes/quotes/p/philipgree622050.html.

56. Jermyn Chow, “SAF Sets up New ‘Cyber Army’ to Fight Digital Threats,” (*The Straits Times*, 2013), http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630.

ME5 Su Juncun is an Air Force Engineer by vocation and is currently serving as an Officer Commanding in 806 Squadron, Air Power Generation Command. He was awarded the SAF Academic Scholarship and graduated with a degree in Mechanical Engineering (Honours, 2nd Class Upper) from the National University of Singapore. ME5 Su's previous appointments included two postings in 6th Air Engineering and Logistics Group, and a staff appointment in Air Engineering and Logistics Department.

The Role of the Military in Cyber Space: Civil-Military Relations and International Military Co-operation

by **Ms Caitríona Heinl**

Abstract:

This article highlights the significance of co-ordination that is key at both the national level within a state and between countries from a strategic and policy perspective for cyber-related issues. It first considers several significant matters that arise in terms of the role of the military and civil-military co-ordination for cyber security. It also highlights a number of challenges in finding the right roles and responsibilities for the military in national cyber security. The article then focuses on military co-operation and dialogue. Finally, it analyses how to ensure that there are mechanisms to prevent further escalation when militaries are involved in managing these threats.

Keywords: Cyber security; Civil-military Relations; Trust; Military Co-operation and Dialogue; Transparency

IMPROVING CIVIL-MILITARY CO-ORDINATION IN CYBER SECURITY[1]

Several important issues can arise for countries in terms of civil-military co-ordination for cyber security, and this accentuates the significance of co-ordination between various agencies within a state. This section will highlight a number of challenges that can arise in finding the right roles and responsibilities for the military in national cyber security. It does so in general terms by identifying common challenges for many countries rather than by providing a country-specific analysis of military strategic approaches. These models can range from countries that adopt a closely integrated civil and military approach, like the Scandinavian countries, to the other extreme where countries adopt a looser co-ordination between the civil and military sectors, such as Germany.[2]

The nature of cyber-related developments has been increasingly affecting traditional civil-military relations to the extent that militaries must consider a number of implications. For instance, (1) cyber capabilities are by nature inherently difficult to verify through arms control mechanisms; (2) the nature of cyber-related threats means that there can be a grey area between criminal and malicious state activity; (3) capabilities are dual-use; and (4) the role of the private sector is crucial. Consequently, several challenges that have arisen for many states include, among others: (1) how to embed cyber security in a nation's public institutions; (2) how to better clarify the exact role of the military; (3) the need for enhanced information-sharing; (4) how to build trust; and (5) managing limited financial and labour resources.

Decision-Making

Cyber-related matters often fall under the purview of several government ministries, and consequently many countries have been working out how to embed cyber security in public institutions over the past few years in order to ensure that responsibilities are clearly defined, bureaucratic stovepipes avoided and co-operation maximised.

For example, several countries have positioned the entity responsible for co-ordinating cyber policy at the highest level like the office of the prime minister or president. One explanation for this is that although military or intelligence services may act in accordance with their own organisational interests, by raising decision-making to such higher levels, interests might then be balanced. These interests include weighing the impact of security policies on the economy and international relations, or weighing the proportionate balance between security and privacy or civil liberty issues.[3]

Better Clarification Of The Role Of The Military

While tensions regarding military involvement in cyber space may arise, the military is a significant stakeholder with an interest in a safe and secure cyber space. Moreover, an increasing number of states are recognising cyber space as a domain for military operations. Nevertheless, while many are currently refining their national cyber security strategies, the military's exact roles and responsibilities in cyber space may sometimes remain unclear. More generally, much attention has instead been focused on acquiring specific technical capacities and expertise to act in cyber space as decision-making procedures, doctrines for deployment and procedures may not always be clearly defined. For such reasons, there is a need to improve strategic decision-making as well as the ability to react to cyber crises.

In most cases, civilian ministries are responsible for co-ordinating incident response and the military is used only as an instrument of last resort. Moreover, in many countries, the military has little or no role in the protection of critical infrastructure. However, it has the responsibility for national defence, which presumably includes defence of the most extreme threats to critical infrastructure. The international community recognises this importance of protecting critical infrastructure. It is described as the backbone of our economies, security and health, and the Internet has become fundamental for the functioning of critical sectors that include energy, telecommunications, transport, health care and banking.[4]

One of the difficulties that might then arise is that where procedures might be outlined in formal doctrines and strategies, such procedures might not always be tested sufficiently in practice. Key players and organisations might still be uncertain about their exact responsibility. Good crisis management and incident response mechanisms should therefore clarify under what circumstances and through which procedures a request can be made for military assistance. In addition, testing these procedures and organisational capacity through realistic exercises should allow for better co-operation in a real crisis situation, and a whole-of-government approach is often recommended.

Public-Private Sector Relations: Enhancing Information Sharing And Trust

The significant role that the private sector has in this field has been particularly challenging for the military and security community. In some cases, a game-changing development has forced the way in which governments (military and intelligence) need to collaborate with the private sector. For instance, (1) militaries are increasingly dependent on civilian critical infrastructure which is becoming more network-enabled; (2) there is greater reliance on commercial products, with exposure to the same vulnerabilities faced by civilians and the private sector; and (3) critical military functions are becoming increasingly cyber-enabled.[5]

The sharing of actionable information on cyber threats and incidents remains a challenge both within many national governments, as well as between the public and private sectors. For instance, while the military and intelligence services may often be unable or unwilling to share classified information, the private sector might also be reluctant to share directly. However, both the public and private sectors require such information for alerts and threat warnings. In addition, this is also an area where recommendations have been made to promote the international exchange of best practices and lessons learned in public-private co-operation.[6]

Trust is important for information sharing, and such trust is often based on personal relationships. Especially since military and civilian cultures can diverge significantly, stakeholders should then develop a system where they meet personally or liaise regularly in order to better understand each other's needs, in order to build a more nuanced understanding of the other's perspectives and responsibilities, and to create points of contact. For example, scheduling weekly calls or monthly meetings can assist in building such relationships and therefore allow stakeholders to be more informed of developments across the field.

From a trust-building perspective, training can be valuable in that it may be applied both cross-sector as well as internationally. For instance, the European Union (EU) Cyber Defence Policy Framework of November 2014 highlights under its section on the promotion of civil-military co-operation that joint activities in the field of training and exercises will enhance co-operation.[7] It further highlights that this could reduce costs across different policy areas. Given the need to manage limited financial resources, this can only be beneficial for countries to consider as an initiative.

Trust is important for information sharing, and such trust is often based on personal relationships. Especially since military and civilian cultures can diverge significantly, stakeholders should then develop a system where they meet personally or liaise regularly in order to better understand each other's needs, in order to build a more nuanced understanding of the other's perspectives and responsibilities, and to create points of contact.

Managing Limited Financial And Labour Resoures

A regular complaint is that not only is there a shortage of cyber security experts, but both the public and private sectors are competing for available talent. More specifically, the recruitment and retention of skilled individuals in the armed forces itself is a challenge common to most jurisdictions. And while this is also the case for the civilian public sector and private sectors, the armed forces faces a particular challenge in attracting and retaining experts given the more profitable civilian domains. Furthermore, while it might be in the military's interests that the best talent be recruited, it also serves the national interest that such individuals are in the industry to support the economy. In addition, while there is a clear shortage of technical expertise, individuals who can translate the implications of technology to strategic choices and policy implications are also relatively scarce.

In order to alleviate this shortage, solutions that have been made include interdisciplinary education, and joint training of military and civilians so as to enhance mutual understanding and create networks of trust. Moreover, in many countries, it is the private sector that supports the military with capacity, products and expertise—therefore the exchange of best practices in recruitment, training and retention, both between the public and private sectors and between international partners, might alleviate these shortages of experts to some extent.

Another issue that states must consider is the management of financial resources and the reduction of costs. Thus, by including industry and academia in exercises, this might mean both the harnessing of a pool of expertise and increased cost efficiencies.[8]

Leveraging Synergies With Other Civilian Actors

For similar reasons, leveraging the capabilities of law enforcement authorities might also mean the harnessing of expertise, and enhanced cost efficiencies. For example, the EU Cyber Defence Policy Framework recommends leveraging existing cyber crime prevention, investigation, and forensic capabilities in the development of cyber defence capabilities.[9] Furthermore, recommendations have been made to leverage law enforcement authorities' expertise by working with armed forces in post-conflict crises or natural disaster situations, where law enforcement might traditionally play a significant role in peacekeeping, capacity building, and reconstruction efforts. Such co-operation could be enhanced to increase cyber capacity building, and the expertise of regional and international law enforcement bodies that assist in building cyber capacity and capabilities might also be leveraged. This is especially noteworthy for the Asia-Pacific region, which is particularly prone to natural disasters.

INTERNATIONAL MILITARY CO-OPERATION, EXCHANGE AND DIALOGUE

This section focuses on military co-operation and dialogue. It analyses how to ensure that there are mechanisms to prevent further escalation when militaries are involved in managing these threats. In

Wikipedia

Soldiers from the United States Marine Corps assisting in disaster relief efforts in the aftermath of Typhoon Haiyan in the Philippines in 2013.

other words, it highlights the importance of ensuring that actions are taken to prevent a possible escalation or conflict that may be sparked by a cyber-related incident. While the military might aim to be prepared to win in conflict, it should also be obliged to avoid escalation.[10] This section thus seeks to elaborate on mechanisms to avoid such escalation, even where the subject is considered sensitive.

If sufficient effort is made to ensure the right mechanisms are implemented to avoid misperceptions and misunderstandings, this article posits that cyber conflict is not inevitable—in the same manner that traditional conflict is not inevitable.

The unique aspects of cyber-related incidents have the potential to cause an escalation to armed conflict. One of the main concerns is the increasing potential for malicious cyber activities by state and non-state actors to create instability and mistrust in international relations. It is therefore important that the military ensures that there is international military-to-military dialogue, exchanges, and co-operation to alleviate possible tensions and prevent the escalation of conflict, especially in an environment where misperceptions could arise. Better forums for dialogue, exchanges and co-operation are needed so that there are mechanisms to prevent further escalation when militaries are involved in managing these threats. If sufficient effort is made to ensure the right mechanisms are implemented to avoid misperceptions and misunderstandings, this article posits that cyber conflict is not inevitable—in the same manner that traditional conflict is not inevitable.

International military-to-military co-operation for cyber-related matters is at a relatively early stage of maturity however, and countries are at different phases of development in this area. Moreover, a fixed structure for international military co-operation is lacking in outside organisations, unlike those within the North Atlantic Treaty Organisation (NATO), and the EU States will also continue to seek to develop or obtain capabilities. Consequently, there is an increasing concern over the lack of military-to-military dialogue in order to prevent miscalculations, misunderstandings, false attribution, or escalation in tensions. This is especially concerning regions, like the Asia-Pacific, where strong interstate tensions exist.

The international community recognises the need for international co-operation to reduce risks, and discussions are focused on reaffirming the applicability of international law to state behaviour in cyber space, as well as the development of voluntary, non-legally binding norms for responsible state behaviour in cyber space during peacetime. In addition, the need to develop and implement confidence building measures (CBMs) to increase stability and prevent the risk of conflict as a result of misperceptions and miscalculations arising from the malicious use of Information and Communications Technologies (ICTs) is recognised.[13]

Promoting More Multilateral And Bilateral Opportunities For Military Exchanges, Dialogue, and Co-operation

Improved international military dialogues, exchanges, and co-operation, whether at bilateral, sub-regional (this could be either inter-regional or intra-regional between like-minded countries), regional, or international levels could lead to better exchange of information to enhance cyber defence effectiveness and international stability.

Lessons learnt relating to processes as well as possible future challenges can be exchanged, and mutually-agreed action points might then be generated. Moreover, this does not need to be limited solely to militaries but can include other stakeholders to enhance international civil-military co-operation.

Such mutually-agreeable action points that could be generated through exchanges and dialogues to facilitate better co-operation are highly important. It is clear that while there is now, in the first instance, a level of agreement by high level officials on the need for states to co-operate as well as on possible areas where co-operation might be needed, currently there seems to be less clarity on specific mutually-agreeable action points and deliverables. Ideally, states should now begin to translate these agreements into real action points for implementation where none already exist.

The issue of trust then becomes significant again and it should not be underestimated in its role in facilitating better co-operation. Officers regularly cite it as key in creating these types of relations. The importance of creating an environment of trust, and enhanced transparency at national as well as international levels to foster an environment of stability needs to be emphasised. In addition, the role of personal relationships in building trust has been cited as very important if incidents arise, especially since problems can take years to resolve. Yet building trust may be easier to highlight and speak of as necessary than it is to achieve in real terms. For example, if there are serious tensions in state relations, it may be extremely difficult to surmount this challenge even when it is recognised as an essential component for enhanced co-operation on cyber-related matters.

Wikipedia

Platforms such as the 2016 ASEAN-US Defence Ministers' Informal Meeting may help facilitate multilateral dialogue and co-operation to foster greater trust.

Soldiers from the Singapore Armed Forces (SAF) and Australian Defence Force (ADF) attending a joint briefing during Exercise Trident in Australia in 2014.

Increasing the levels of transparency is also regularly highlighted by government officers as key to ensuring an environment of stability as well as for developing common concepts in this domain. Such points are highly significant when there are recent concerns that are currently being echoed over an increasing environment of mistrust, especially in the Asia-Pacific region. Lastly, where possible, more effort should equally be made to ensure that there is better co-ordination and co-operation between initiatives across international and regional platforms. This should then create enhanced complementarity and avoid duplication of efforts.

A recent example from May 2015 of an initiative to increase co-operation in this area is that of the EU's Estonia-Latvia Presidency Cyber Hygiene Initiative proposed by two smaller EU Member States to increase awareness of and promote the need for basic cyber security standards within defence organisations covering human-related risk factors (this has apparently been a factor in more than 80 per cent of cyber incidents reported).[17]

Confidence Building Measures

Ideas derived from more traditional military-to-military CBMs like official military-to-military contact points and crisis communication procedures such as hotlines could assist in increasing such transparency, and reducing the risk of misperception in state behaviour and unwanted escalation. Stakeholders have suggested that existing common understanding, trust, and shared interests can also be built upon in order to enhance transparency and co-operation. Ultimately, this could then assist in strengthening existing structures or establishing structures where none exist in order to allow for stronger collaboration in future.

Where appropriate, there needs to be an increase in the level and regularity of military-to-military consultations and dialogue, information sharing on strategies, policies and institutional structures, joint exercises, as well as practical collaboration through bilateral or multilateral platforms. This further contributes to building mutual understanding and confidence. The exchange of information and best practices alone can help build trust as a starting point and prevent misunderstanding. For instance, while cyber security and cyber defence strategies may be quite different, their predominant role is the setting of goals and determining the means to achieve these goals, and such strategies have a strong declaratory function vis-a-vis other states. The right strategy can therefore present an opportunity to reduce the risk of conflict.

Small-step, military-to-military dialogues and other practical co-operation measures could additionally complement this objective of building confidence and improving international stability through international political agreement.

In terms of the current status of discussions over cyber, the exchange of national definitions or key terminology can further assist in building better understanding between parties and in alleviating the potential for misunderstandings between states. It has been suggested that an index or glossary of terms could even go some way to achieving this common understanding.

While pursuing international agreement on state behaviour in cyber space is desirable, there is still further space for possible progress by practical military-to-military dialogue or co-operation (as well as international civil-military co-operation) on cyber issues. Small-step, military-to-military dialogues and other practical co-operation measures could additionally complement this objective of building confidence and improving international stability through international political agreement.

States are therefore being encouraged to be more transparent about the roles and responsibilities of their defence forces and security services in the cyber domain as well as to pursue dialogue and other measures related to cyber issues to build confidence and ensure international stability.[19]

CONCLUSION

Although many of these points may not seem overtly new, they have not yet been fully resolved. This field is an evolving work in progress. In short, the principles of trust, transparency, and co-operation should be integrated within the majority of portfolios since there are few areas where cyber or ICT are not relevant. This is particularly important in order to mitigate the probabilities of escalation occurring on account of the nature of this field.

ENDNOTES

1. Heinl & Boeke, "Civil-Military Relations & International Military Cooperation in Cyberspace", University Leiden Campus the Hague, Research Project supported by The Netherlands Ministry of Defence, April 2015. Much of the material in this section is from this research project conducted in April 2015. The paper identified a non-exhaustive list of ongoing common global challenges and possible good practice solutions for a more effective response. In doing so, the paper reflected non-prescriptive inputs from a wide spectrum of global civil-military stakeholders including civilian agencies, the defence forces, academia and the private sector that emanated from an informal roundtable held in Singapore in November 2014.

2. Centre of Excellence for National Security Cybersecurity Workshop, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Conference Report, Singapore, 20-21 July 2015.

3. This article does not outline the structure of decision-making at national level in Singapore. Rather it considers the more general challenges facing a majority of nation states in this field. In addition, in the past year a number of agencies have been established that house cyber expertise from across governments so as to coordinate the efforts of the civilian and military agencies.

4. Chair's Statement, *Global Conference on Cyberspace 2015*, n._20/21, 17 April 2015.

5. Centre of Excellence for National Security Cybersecurity Workshop, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Conference Report, Singapore, 20-21 July 2015.

6. Chair's Statement, *Global Conference on Cyberspace 2015*, n._20, 17 April 2015.

7. Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14, 18 November 2014, 8.

8. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

9. Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14, 18 November 2014, 8.

10. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

11. Chair's Statement, *Global Conference on Cyberspace* 2015, n._29, 17 April 2015.

12. Chair's Statement, *Global Conference on Cyberspace 2015*, n._30, 17 April 2015.

13. Ibid.

14. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace* 2015, 17 April 2015.

15. Author's observations, *ASEAN Regional Forum Workshop on Cyber Security Capacity Building*, Hosted by the People's Republic of China and Malaysia, Beijing, 29-30 July 2015.

16. Ibid.

17. Centre of Excellence for National Security Cybersecurity Workshop, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Conference Report, Singapore, 20-21 July 2015.

18. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

19. Chair's Statement, *Global Conference on Cyberspace 2015*, n._38, 17 April 2015.

20. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

Caitríona Heinl Caitríona Heinl joined the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies as a Research Fellow responsible for cyber analysis in October 2012. She has published peer-reviewed articles as well as both public and government policy advisory reports on topics that include engagement on emerging cyber challenges, international security and international cyber policy research, national security implications of emerging technologies. She currently holds a non-resident international fellowship with the Australian Strategic Policy Institute International Cyber Policy Centre, Canberra.

Ms Heinl previously led the Justice and Home Affairs policy group and Justice Steering Committee at the Institute of International and European Affairs (IIEA), Ireland. She qualified as a Solicitor in the UK (non-practising) and has been admitted as an Attorney-at-Law in New York. She is currently a member of the Irish government's Department of Foreign Affairs and Trade Foreign Policy Network.

Ms Heinl holds a Masters of Philosophy in International Relations from the University of Cambridge, having graduated in both commerce and law at University College Dublin and the Leopold Franzens University of Innsbruck in Austria with 1st Class Honours.

Technologies Converge and Power Diffuses

by **Dr. Thomas X. Hammes**

Abstract:

The convergence of dramatic improvements in the fields of robotics, artificial intelligence, materials, additive manufacturing and nano-energetics is dramatically changing the character of conflict in all domains. These developments will provide smaller powers—and even some individuals—with capabilities that used to be the preserve of major powers. This diffusion of power has major implications on the conduct of warfare and national strategy. This is because while massive investment in mature technology leads to only incremental improvement in capabilities, the proliferation of many small and smart weapons may simply overwhelm a few exceptionally capable and complex systems. Strategically, small nations will be able to afford effective anti-access/area denial (A2/AD) defences that can defend not only their territories, but also reach out to strike an invader's intermediate and home bases. They can generate many of the capabilities of the most expensive current systems at a fraction of the cost, which will drastically change the calculus of intervention. However, the critical military functions will remain—but how they will be accomplished will change. Rather than investing everything in few, exquisite and very expensive systems, it makes more sense to explore augmenting them and, in time, replacing them with systems that conform to small, smart, and many.

Keywords: Additive Manufacturing; Nano-energetics; Changing Character of Conflict; Investment in Mature Technology; Small and Smart Weapons.

HISTORICAL CASE

Fortunately, this level of technological change and convergence is not unprecedented. From 1914 to 1939, there were breakthroughs in the fields of metallurgy, explosives, steam turbines, internal combustion engines, radio, radar, and weapons. In 1914, at the beginning of World War I (WWI), battleships were considered the decisive weapon for fleet engagements, and the size of the battle fleet was seen as a reasonable proxy for a navy's strength. The war's single major fleet action, the Battle of Jutland, seemed to prove these ideas correct. Accordingly, during the interwar period, battleships received the lion's share of naval investments. Navies took advantage of rapid technological gains to dramatically improve the capabilities of the battleship. Displacement of capital ships almost tripled, from the 27,000 tons of the pre-WWI United States (US) *New York* class to the 71,660 tons of Japan's *Yamato* class. The largest main batteries grew from 14-inch to 18-inch guns with double the range. Secondary batteries were improved, radar was installed, speed increased from 21 to 33 knots for US fast battleships, cruising range more than doubled, and armor improved. Yet, none of these advances changed the fundamental capabilities of the battleship—they simply provided incremental improvement on existing strengths. This is typical of mature technology, even massive investment leads to only incremental improvement(s).

In contrast, naval aviation was in its infancy in 1914. Aircrafts were slow, short-legged, lightly armed, and used primarily for reconnaissance. Air combat was primitive—one early attempt at this endeavour involved a grappling hook! Military aviation made great strides in tactics, technology, and operational concepts during the war. Yet, after the war, aviation—particularly naval aviation—remained an auxiliary and was funded accordingly. The US and United Kingdom (UK) governments focused most of even this limited investment on heavy bombers. Despite this neglect, by 1941, carrier aviation in the form of fighters, dive bombers, and torpedo bombers dominated Pacific naval warfare. Most of the advances in aircraft design and production that applied to naval aviation were developed for civilian uses. Aircraft production was a wide-ranging and highly-competitive business that led to these rapid technological advances. Relatively modest investment in these new technologies resulted in massive increases in aircraft capability. As a result, in World War II (WWII), aircrafts—the small, smart, and many weapons of WWII naval force—could swarm and destroy the few and exquisite battleships. By mid-1942, the battleships were reduced to expensive anti-aircraft and naval gunfire platforms.

Yet, none of these advances changed the fundamental capabilities of the battleship—they simply provided incremental improvement on existing strengths. This is typical of mature technology, even massive investment leads to only incremental improvement(s).

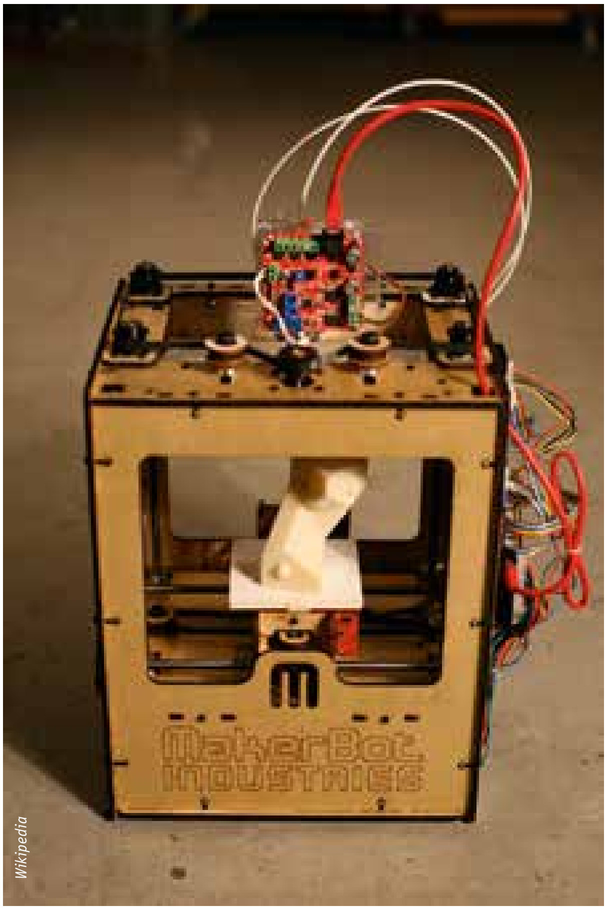
However, it is important to note that the transition took almost 20 years. Thus, the early investment in battleships was correct. The failure lies in not understanding when the character of naval warfare changed and naval aviation capabilities exceeded those of the battle line. Interestingly, there was also relatively little investment in submarines, the other powerful newcomer to the naval battle. Submarines progressed from a fragile but deadly weapon system in WWI to one that almost defeated Britain and destroyed the Japanese industry in WWII. It is essential to remember that institutional biases can keep investment focused on the dominant technology even as multiple emergent technologies clearly challenge it.

EVOLVING TECHNOLOGIES

As noted in the introduction, we are currently in an area of rapidly evolving technologies that, when combined, may well radically alter the way we fight. This paper is too short to even begin to explore the explosion of new technologies that are changing our daily lives. However, it will take a look at a few that will have short-term impact on how wars are fought—additive manufacturing, nano-materials and energetics, space-like capabilities, artificial intelligence, and drones. This paper will also consider how they may come together to change conflict.

Additive Manufacturing

In the last few years, additive manufacturing (AM), also known as 3D printing, has gone from an interesting hobby to an industry producing a wide range of products from an ever growing list of materials. The global explosion of AM means it is virtually impossible to provide an up-to-date list of materials that can be printed, but a recent top ten list includes metals such as stainless, bronze, steel, gold, nickel steel, aluminum, and titanium; carbon fibre and nano-tubes; stem cells; ceramics; and food.[1] In addition to a wide range of materials, AM is progressing from a niche capability that produces prototypes to a manufacturing industry capable of producing products in large quantities. United Parcel Service (UPS) has created a factory with 100 printers.[2] The current plant requires one operator per



A MakerBot three-dimensional printer.

eight-hour shift and works around the clock. It accepts orders, prices them, prints them and ships them on the same day from its adjacent shipping facility. With 100 printers, UPS can print production runs of a number of products, and the firm has plans to increase the plant to 1,000 printers to support major production runs.

At the same time, AM is dramatically increasing the complexity of objects it can produce while simultaneously improving speed and precision. Recent technological developments indicate that the industry will be able to increase 3D printing speeds up to 100 times with a goal of 1,000 times, all while providing higher quality than current methods.[3] In January 2015, Voxel8 revealed a new printer ($8,999) that printed a complete, operational drone with electronics and engine included.[4] In February 2015, Australian researchers printed a jet engine.[5] Furthermore, the very nature of additive manufacturing reduces the price of parts since there is little or no waste. With subtractive (or traditional) machining, one starts with a block of metal and cuts it to the correct form, wasting a great deal of material. With AM, material wastage is near zero, thus making it cheaper to make a part from titanium using AM than from steel using traditional machining. Although only two decades old, AM is already starting to encroach on a wide range of traditional manufacturing.

Nano-Technology

Nano-technology is another field that is advancing rapidly in many areas, two of which are of particular interest to us. The first is nano-energetics or explosives. As early as 2002, nano-explosives generated twice the power of conventional explosives.[6] Since research in this field is close hold, it is difficult to say what progress, if any, has been made since that point. Obviously, it would be unusual if greater efficiencies have not been achieved in over a decade. But, even if two times is as good as it gets, a 100 percent increase in destructive power for the same size weapon is a massive increase. Much smaller platforms will carry greater destructive power. The second area is nano-materials. Although this field has not advanced as far as nano-energetics, the potential for nano-carbon tubes to dramatically reduce the weight needed for structural strength will have significant implications for an increasing range of drones. In a related field, numerous firms are applying nano-materials to batteries and increasing their storage capacity.[7] In fact, a recent accidental discovery may triple battery power storage and increase battery life by a factor of four.[8] Researchers are also applying nano-technology to develop capacitors that can function as batteries.[9] These improvements in energy storage, materials, and explosives will lead to increases in range and payload for a wide variety of vehicles.

Space-Like Capabilities

The addition of cheap persistent space-based and air-breathing surveillance will provide the information necessary to employ these new technologies. In space, several companies are deploying cube satellites (CubeSats) in order to include SkyBox Imaging which was recently purchased by Google. Their goal is to sell half-metre resolution imagery with a revisit rate of several times a day—to include an interpretation of what the buyer is seeing.[10] A buyer could literally track port, airfield, road, rail system activity in near real time. Initially, SkyBox and other CubeSats companies achieved low-cost launch by serving as ballast on larger rockets. Today, New Zealand's Rocket Lab is proposing to conduct weekly launches specifically for CubeSats to allow rapid, cheap launch of CubeSats. Although Rocket Lab has not yet opened its space port, numerous firms have signed up for its launch services.[11]

Other firms are working on systems that can duplicate the communications and surveillance functions provided by satellites. Google's Project Loon is attempting to provide reliable, cost-effective internet services for much of the southern hemisphere by deploying a constellation of balloons that will drift in the stratosphere.[12] High-altitude long-endurance drones are another avenue to satellite capabilities without the satellite. The US Air Force has successfully tested Global Observer to conduct surveillance and intelligence operations.[13] For long endurance operations, several organisations are pursuing solar-powered drones.[14]

Artificial Intelligence

Artificial intelligence (AI) is yet another exploding field, but two areas are of particular importance in the evolution of small, smart, and cheap weapons—navigation and target identification. Global Positioning System (GPS) has proven satisfactory for basic autonomous drone applications such as the Marine Corps K-MAX logistics helo-drone in Afghanistan.[15] However, GPS will be insufficient for operations in narrow outdoor or indoor environments, dense urban areas, and areas where the GPS signal is jammed. Academic and commercial institutions are working hard to overcome the limitations of GPS to provide truly autonomous navigation for drones.[16] Inertial and visual navigation are advancing rapidly and are already cheap enough to use in small agricultural drones.[17] Clearly, the commercial applications for navigating in agricultural areas and inspecting buildings in urban areas can be adapted for military uses. While such a system would serve to get a drone to the target area, it would not ensure that a specific target could be hit. For that, optical recognition is essential. And in fact, there have been major advances in surveillance and tracking software that are more than sufficient for an autonomous drone to attack specific classes of targets and perhaps even specific targets.[18] Today, artificial intelligence can identify a distinct object—such as an aircraft or fuel truck—using on board multi-spectral imaging.[19] In short, the AI necessary for many types of autonomous drone operations currently exists—and is operating aboard small, commercial drones.

AI is the development that makes the convergence of material, energetics, drones and additive manufacturing such a dangerous threat. It is advancing at such a rapid rate that over 1,000 distinguished researchers signed an open letter seeking to ban autonomous weapons. They stated that "the deployment of such systems is, practically if not legally, feasible within years, not decades..."[20] It is exactly that autonomy that makes the technological convergence a threat today. Because such drones will

Cyberpioneer

The future of the Singapore Armed Forces (SAF) will utilise more unmanned systems and drones, as shown during the Future of Us exhibition.

require no external input other than the signatures of the designated target, they will not be vulnerable to jamming. Not requiring human intervention, they will be able to operate in very large numbers. They can be programmed to wait patiently prior to launch or even proceed to the area of the target, but hide until a specified time or a specified target is identified.

Drones

Clearly, drone capabilities have increased dramatically in the last five years and, perhaps most significantly, usage has spread widely. Still, small drones can only carry a limited payload. This limitation can be overcome with two separate approaches, one of which is the use of Explosively Formed Penetrators (EFPs). The other less technically challenging approach would be to think in terms of 'bringing the detonator'.

For harder targets, EFPs will allow even small drones to damage or destroy armoured targets. Weighing as little as a few pounds, these penetrators can destroy even well-armoured vehicles. In Iraq, Coalition forces found EFPs in a wide variety of sizes—some powerful enough to destroy an Abrams tank. Others were small enough to fit in the hand—or on a small drone.[22] And of course, nano-explosives at least double the destructive power of the weapons.

The primary limitation on production in Iraq was the need for high-quality shaped copper plates that form the projectile when the charge is detonated. Up until recently, this was a significant challenge that required a skilled machinist with high quality machine tools. However, in the last few years, additive manufacturing has advanced to the point that it can be used to print a wide variety of materials to include copper.[23] The US space agency, National Aeronautics and Space Administration (NASA), has printed a copper combustion chamber liner for a rocket motor.[24] Thus, we can expect small and medium-sized drones to pack a significant punch against protected targets.

The second approach entails bringing the detonator, and it applies to aircraft, vehicles, fuel, and ammo dump targets. In each case, the objective is to simply detonate the large stock of explosive material already provided by the target. Against these targets, even a few ounces of explosives delivered directly to the target can initiate the secondary explosion that will destroy the target.

The convergence of new technologies discussed above may allow these small, smart, and cheap drones to dominate combat in the land, air and sea domains. Anyone with a television or access to YouTube during the last decade will be very familiar with the US' use of drones to both hunt enemies and protect friendly forces. Although the numbers stand in the tens of thousands worldwide, these drones represent only the first wave. Like many technologies, early versions were expensive and difficult to operate, thus only the wealthy employed them. But over time, technology has become cheaper, more reliable and is more widely employed. We are seeing this with the explosive growth in commercial drones. Indeed, additive manufacturing will soon make them cheap enough for small companies and even individuals to own a large swarm of simple, autonomous drones.

In fact, the US Air Force is actively exploring the use of swarms, with most of its focus on smart swarms that communicate and interact with each other and other platforms.[25] The US Navy is also pursuing swarming technology with the Low-Cost Unmanned Aerial Vehicle Swarming Technology (LOCUST) as well as small craft.[26] While these programmes are vague about how many drones will be involved, they envision being able to employ large numbers as recent, dramatic cost reductions in each of the needed technologies will increase the number by a sizeable magnitude. Researchers in England have prototyped a simple drone body that costs roughly US$9 a copy.[27] Researchers at the University of Virginia are 3D printing much more complex drones in a single day, then adding an Android phone to produce a US$2,500 autonomous drone.[28] Thus, a small factory with only 100 3D printers using the new printing technology noted above could produce 10,000 drones a day. The limitation is no longer the printing, but the assembly and shipping of products. However, both processes can be automated with industrial robots. Then, the limitation becomes preparing and launching thousands of drones at a time when they arrive in theatre, which will require refined organisation, planning, and equipment.

The limitation is no longer the printing, but the assembly and shipping of products. However, both processes can be automated with industrial robots. Then, the limitation becomes preparing and launching thousands of drones at a time when they arrive in theatre, which will require refined organisation, planning, and equipment.

Nor will cheap drones be limited to the air. In 2010, Rutgers University launched an underwater 'glider' drone that crossed the Atlantic Ocean unrefueled.[29] Such drones are being used globally and cost about US$100,000.[30] This year, the US Navy launched its own underwater glider that harvests energy from the ocean thermocline and they are planning to operate it without refueling for five years.[31] Based on the commercially produced Slocum Glider—a five-foot long autonomous underwater research vehicle—it can patrol for weeks following initial instructions, then surface periodically to report and receive new instructions. In short, small sea platforms have demonstrated the capability of achieving intercontinental range while producing very little in the way of signatures.

Ashore, mobile land mines/autonomous anti-vehicle weapons are also under development.[32] The natural marriage of Improvised Explosive Devices (IEDs) to inexpensive, autonomous drones is virtually inevitable. However, truly autonomous land drones—those that actually move on the ground—will remain the most difficult challenge simply because land is the most complex combat environment. Thus, AI and maneuvering for land drones require an order of magnitude for far more capability than for air or sea. In the interim, cheap fixed and rotary wing drones will provide an inexpensive way to strike ground targets. Non-state and state actors alike can rapidly transition to drones that can hunt mobile targets.[33]

IS IT EVEN POSSIBLE TO LAUNCH THOUSANDS OF DRONES?

It is one thing to have access to thousands of drones, it is quite another to have the logistics and manpower available to effectively employ them. One method that demonstrates it can be done is the Chinese system that mounts 18 Harpy Unmanned Combat Air Vehicles (UCAVs) on a single five-ton truck using a system similar to a Multiple Launch Rocket System (MLRS).[34] The Chinese can transport, erect, and fire these fairly large drones with a single vehicle and a one or two-person crew. Initially developed in the 1990s by Israel as an anti-radar system, the Chinese version has a range of 500 km and a warhead of 32kg with multiple types of seeker heads. Both China and

Wikipedia

The British M270 Multiple Launch Rocket System (MLRS) firing a rocket during an exercise. The M270 is the original version of the MLRS, which features a weapon load of 12 rockets in two six-pack launch pod containers.

Israel have displayed these weapons at trade shows in an effort to sell them to other nations. The system is currently operational with the Turkish, Korean, Chinese, and Indian armies. Today, the Israeli version, the Harop or Harpy 2, has an electro-optical sensor to attack non-emitting targets and an extended range of 1,000 km.[35] One can assume that China has made similar improvements to its systems. Thus, even with old technology, the capability to launch swarms of drones already exists. Further, the Harpy is not a small weapons system. A similar-sized vehicle could be configured to carry over 100 Switchblade size drones or perhaps a thousand mini-drones.[36]

IMPLICATIONS FOR THE MODERN BATTLEFIELD

Irregular War

Unfortunately for nation states, autonomous drones will initially favor the less technologically advanced actor because their targeting problem is simpler. For instance, a non-state actor may not own armoured vehicles or aircrafts, so their autonomous drones only have to find and attack any armoured vehicle or parked aircraft. It does not have to discriminate but simply fly a pre-programmed route to a suspected target area. Target areas for many locations in the world—to include most airfield flight lines—can be determined using Google Maps or Google Earth. Cheap optical recognition hardware and software that provide effective target discrimination are also becoming widely available. Thus, once in the target area, the drone can scan for an easily identifiable target, say a large cargo aircraft, and then simply crash into it. Limited standoff is also currently available. If the software of a farmer's autonomous drone can point and shoot a camera, it can point and shoot a projectile as well.

Soon, Skybox Imaging or similar firms will provide near real-time imagery to anyone with a credit card and a laptop. Terrorists and insurgents will be able to conduct initial target studies without leaving their houses. Using Tor and the current version of the Silk Road dark website, they will be able to purchase the systems too.

Clearly, today's commercial products have demonstrated the ability for autonomous drones to reach a target area, but what weapon could it use? Against the thin skin of an aircraft, a simple point-detonating three-ounce warhead would be sufficient. Thus, even very small commercial quadcopters can destroy an aircraft on the ground. Against armour, the drone designer may choose the heavier and more complex, explosively formed penetrator. This will obviously require larger quadcopters/drones, but they will also help provide standoff distance. Like most commercial products, for more money, you can purchase more capability in terms of payload, range and discrimination. Advances in additive manufacturing, composite materials, energy densities in gel fuels, and nano-explosives indicate that we will be able to build longer range, more powerful and stealthier drones in the immediate future. Unfortunately, almost all of our anti-terror physical defenses are based on blocking observation and ground access to targets. Drones will simply fly over existing defences. Defending against this threat is a possibility but expensive, particularly when the cost of defending against these weapons is compared to the cost of employing them.

In theatre, top-down attack drones will negate the gains that the West has made in survivability against ground IEDs. Even Mine Resistant Ambush Protected (MRAP) and light armoured vehicles will no longer protect our people or supplies. The fact that fuel and water trucks are distinctive and vulnerable creates more trouble. A smart enemy may well ignore your combat forces and literally fly over them to attack your logistical forces. Operationally, how do you protect ports of debarkation and logistics nodes? How do we defend intermediate supply depots? Overhead cover will work, but also dramatically increase the time, resources and effort that must be dedicated to logistics support. And, of course, the supply vehicles remain vulnerable while loading and transporting those supplies.

And, for the first time in history, insurgent groups may well be able to purchase weapons that can project forces well outside the area of conflict. Very long-range drone aircraft and submersibles give an insurgent the capability to strike air and sea ports of debarkation, and perhaps even embarkation. This will create major political problems in sustaining a US effort. For instance, a great deal of our support into Iraq flows through Kuwait. Suppose the Islamic State of Iraq and Syria (ISIS) demonstrates to Kuwait that it can deploy drones that can hit an airliner sitting at Kuwait International Airport. They state they will not do so as long as Kuwait withdraws landing rights for those nations supporting Iraq. Similar threats can also be made against sea ports. When the time comes, is the West prepared to provide the level of air defence required to protect key targets across those nations providing interim bases and facilities?

Conventional War

While these systems pose a genuine threat to all nation states, they and their descendants will provide a significant boost to the ability of small and medium states to defend themselves. This may lead to a period similar to that between 1863 and 1917 where any person or animal moving above the surface of the ground could be cheaply targeted and killed. Thus, defence has become the dominant form of ground warfare. Drone swarms may make defence the dominant form of warfare in ground, air, sea, and space domains. Drone swarms will also be able to attack the physical elements of the cyber domain. The advantage will come to those who can exploit the domains while operating from a heavily-defended and fortified position.

Ground Domain

The performance of American and British armoured forces in Operations Desert Storm and Iraqi Freedom shows how well-trained crews with advanced gunnery systems could make short work of poorly trained crews in less capable tanks. It seemed that the combined arms team in the offensive was dominant on the battlefield. Then, the 2006 Israeli-Hizbollah war indicated that well-trained, determined irregulars armed with advanced anti-tank weapons, particularly guided missiles, could make defence dominant again in ground warfare. Since then, conventional ground warfare has become both deadlier and cheaper. Direct fire gunnery systems have improved, wire-guided and fire-and-forget missiles systems are proliferating, but both are very expensive. In contrast, artillery can now provide much cheaper precision fire. While each Excalibur 155mm round costs about US$100,000, the US Army signed a contract in 2015 for a new 155mm fuze that makes any 155mm artillery round a precision weapon.[37] Each fuze costs only about US$10,000.[38]

The next great leap will be inexpensive drones. For much less that the price of a precision fuze, commercially available autonomous drones will provide greater range than artillery without the latter's large logistics and training tail. Deployed in large numbers, these drones will provide a particularly nasty challenge for ground forces. Autonomous drones which have already demonstrated the ability to use multi-spectral imagery to identify specific objects, will hunt on their own.

Today, even relatively light forces are dependent on vehicles and helicopters for support. For over a decade, western forces have struggled with hunting

IEDs to ensure the ability to move about the battlespace. Now, the IEDs will start actively hunting our forces in the field, our vehicles, our helicopters and our fuel and ammo dumps.[39] When one combines simple drones with additive manufacturing, ground forces face the real possibility of thousands of drones in wave attacks.

Autonomous drones will be the most difficult to defeat, but remote control drones will most likely appear first. Yet even remote-controlled drones no longer require the operator to have line of sight to his target. Today, even hobbyists are using immersion goggles to control high speed, maneuvering drones.[40] As mentioned earlier, autonomous drones that operate on the ground will be the most difficult to defeat, but they will arrive, and early versions may simply be self-deploying mines/IEDs. Later versions may be advances on the Fire Ant and will be capable of actively hunting ground targets.[41] This has major implications on everything from force structure to equipment purchases to operational and tactical concepts. Tactically, how does a force protect itself against swarms of thousands of small, smart, cheap drones?

Sea Domain

Obviously, swarms of autonomous drones provide a challenge to any naval force trying to project power ashore. The drones need not attempt to sink a ship, but only achieve a mission kill. For instance, a drone detonating against an aircraft on the deck of a carrier or firing a fragmentation charge against an Aegis platform's phased-array radar will degrade its capabilities. While the self-defence systems and speed of most warships make them difficult targets, amphibious or cargo ships have to slow down or stop to operate and thus will be easier targets. And, of course, with drones achieving trans-Atlantic range already, home ports must now be defended.

Undersea weapons will provide a much greater challenge to navies. There is clearly a movement by middle powers in Asia to establish effective submarine forces. However, a submarine force is expensive, complex and difficult to operate. Unmanned underwater vehicles may provide a much cheaper alternative for a middle power. This year, the US Navy has launched an autonomous underwater glider with plans for it to operate for five years without refueling.[42] Similar drones are being purchased globally for about US$100,000 each but commercial firms are striving to reduce the cost by 90 percent.[43] If developed as a weapons system, they could dramatically change the face of naval combat. Offensively, they can become self-deploying torpedoes or mines with trans-oceanic range. Defensively, they can be used to establish smart minefields in maritime choke points. They can be launched from various surface and subsurface platforms or even remain ashore in friendly territory until needed, during which they will be launched from a port or even the beach. Imaginatively, they could be a relatively inexpensive substitute for a submarine force. Clearly, such drones can be modified to be long-range autonomous torpedoes or even to position smart mines. For the cost of one Virginia-class submarine, a nation could purchase 17,500 of such drones at current prices.[44] If additive manufacturing can reduce the cost of these systems roughly by 40 percent that is predicted for satellites, one could buy almost 30,000 such drones for the current cost of a Virginia-class submarine.[45] What is more important is that the skills and organisation needed to build and employ a glider are orders of magnitude less than those needed for a nuclear sub.

Sea mines should be a particular concern to trading nations. They have the distinction of being the only weapon that has denied the US Navy freedom of the seas since WWII. First, mines defeated a US amphibious assault: the landing at Wonson in 1950.

While lanes were eventually cleared through the primitive minefields, forces attacking up the east coast of Korea had already seized the amphibious objectives before the first amphibious forces got ashore. After Wonson, the commander of US Naval Forces noted that the most powerful navy in the world was stopped by weapons designed 100 years ago and delivered by ships designed 2,000 years ago. However, not much has changed. In February 1991, the US Navy had its operations in the northern Arabian Gulf jeopardised by the over 1,300 simple, moored mines that were sown by Iraqi forces.[46]

Since 1950, mines have become progressively smarter, more discriminating and more difficult to find. They have sensors which can use acoustic, magnetic and other signals to attack a specific kind of ship.[47] As early as 1979, the United States fielded encapsulated tornado (CAPTOR) mines. These are basically encapsulated torpedoes anchored to the ocean floor. When they detect the designated target, they launch the enclosed torpedo to destroy it up to a range of eight kilometres.[48] Today, China possesses 'self-navigating mines' and even rocket-propelled mines.[49] We are seeing early efforts to use unmanned underwater vehicles to deliver mines. Since

Wikipedia

A Polish contact mine. When deployed, the protuberances near the top of the mine will trigger the mine's detonation upon contact with any ships out at sea.

commercially-available drones are already crossing the ocean autonomously, pairing drones with mines will most certainly make it possible to mine sea ports of debarkation and perhaps even sea ports of embarkation as well as sea lines of communication.

And, of course, these gliders can also be used against commerce. Launched from shore bases, these systems will allow any nation bordering the South China Sea and its critical straits to interdict trade. While they cannot stop trade, damaging a few ships will cause dramatic increases in maritime insurance rates. To date, no nation has developed a minehunting force capable of clearly smart, self-deploying mines with a high degree of confidence.

Air Warfare

For air warfare, the key problem will be protecting aircraft on the ground. An opponent does not have to fight modern fighters or bombers in the skies. Instead, he can send hundreds or even thousands of small drones after each aircraft at its home station. Tanking, airborne early warning, transport and other support aircraft are even more difficult to protect on the ground. Even if aircrafts are protected by shelters and radars, fuel systems and ammunition dumps are still highly vulnerable. Currently, range is a problem for printed drones, but an Aerovel commercial drone first crossed the Atlantic in 1998 and the company now sells an extremely long-endurance drone.[50] The exceptionally rapid increases in commercial drone capabilities indicate range problems will soon be solved, even for markedly smaller drones.

While manned aircraft will become vulnerable due to basing issues, cruise missiles will become both more capable and cheaper. According to the

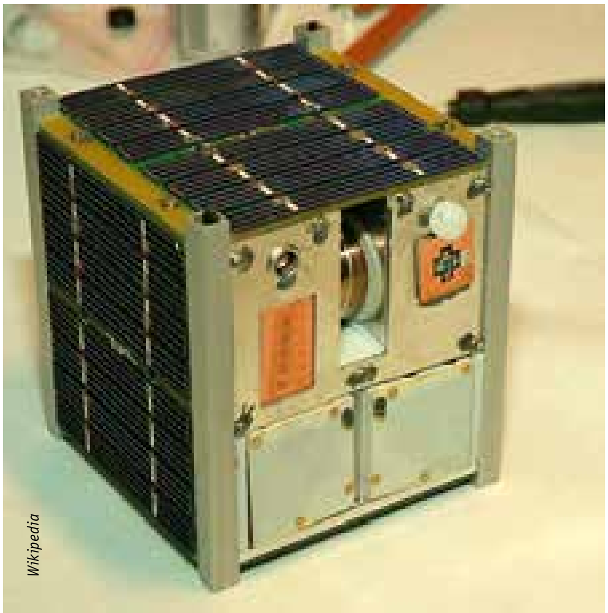
Wikipedia

A Tomahawk Land Attack Missle (TLAM) detonating above its test target.

Naval Air Systems Command, the older Tomahawk Land Attack Missile (TLAMs) cost US$607,000 in FY-99 dollars.[51] Today, that cost stands at $785,000 in FY-2013 dollars.[52] As noted earlier in this article, Lockheed expects to be able to cut the cost of two new satellites by 40 percent using AM. This has some very interesting implications for reducing cost of complex systems. If we assume we can obtain production savings similar to those projected for the satellites, TLAMs will cost about US$470,000 each. These missiles carry a 1,000-pound warhead for a distance of up to 1,500 miles (Block II variant).[53] While somewhat expensive, missiles such as these can provide long-range heavy strike—particularly if the warhead uses nano-explosives. Since they can be fired from a variety of land and sea launchers, they can either be dispersed or hidden in underground facilities (to include commercial parking garages) until minutes before launching. Thus, missiles will remain immune to most pre-emptive strikes and still cost less than ballistic missiles.

The key question is whether we will invest in the equivalent of battleships or aircrafts. Will our investments prove to be exquisite and irrelevant or change the face of conflict?

The previously mentioned US Air Force experiments that uses cargo aircraft to launch dozens of drones also has some very interesting implications for the future of airpower. The combination of cheap drones and much more capable cruise missiles may offer small and medium-sized states A2/AD, precision-strike and long-range strike capabilities in the air domain.


Wikipedia

Ncube-2, a Norwegian CubeSat.

Space Warfare

In space, the advent of micro and cube satellites paired with commercial launch platforms will allow a middle power to develop an effective space programme for surveillance, communications, navigation and even attack of other space assets. In addition to Skybox Imaging and Rocket Lab, Japan's Axelspace is also launching CubeSats. In Axelspace's case, it has launched a US$1.9M satellite to provide navigation assistance in the Arctic. It plans to launch a constellation of CubeSats similar to Skybox Imaging's that will provide hourly satellite imagery of Tokyo's traffic.[54] As such, surveillance and navigation satellites are already within reach of a small or medium power or, it can buy the service from a commercial company.

In addition, high-altitude, long-endurance (able to stay in the air for months) drones and even balloons are being tested by a number of commercial firms as alternatives for providing internet connectivity and surveillance. The British Ministry of Defence is studying the Zephyr 8, a solar power drone that can fly at altitudes up to 70,000 feet and provide surveillance and communications at a fraction of the cost of current satellites.[55]

Cyber Warfare

While one would not normally think of drones as part of conflict in cyber space, it is important to remember that all networks have nodes in the real world. Furthermore, some of these nodes such as key fibre-optic network lines and switches are quite exposed. For instance, satellite downlinks and point where fibre-optic networks come ashore are both exposed and vulnerable. Smart drones provide a way to attack these nodes from a distance.

Offering more potential for precision effects, Boeing successfully tested its Counter-electronics High-Powered Advanced Missile Project (CHAMP) in 2012. CHAMP is a drone mounted Electro-magnetic Pulse (EMP) system that successfully knocked out all electronic targets during its test.[56] Such a system can target specific nodes of an enemy's network while not damaging friendly nodes.

STRATEGIC IMPLICATIONS

Since Operation Desert Storm, there has been a belief that information superiority tied to precision weapons will defeat mass. It has certainly allowed numerically smaller Allied forces to defeat Iraq's much larger Army (twice) as well as drive Al Qaeda and the Taliban out of Afghanistan using a very small ground force. However, the convergence of several new technologies seems to be pointing to the revival of mass (in terms of numbers) as a key combat multiplier. The small, smart, and many revolutions will provide all nations and some non-state groups with capabilities previously reserved for great powers simply because they cost so much.

Western forces have had the luxury of unopposed access to the theatre of operations outside Europe for decades. This monopoly is changing as US access will be contested in several domains. We have to ask the question 'Does the strategic cost/benefit calculation change as a result?' When almost any enemy can cause severe damage throughout a major power's supply, deployment and employment chains—perhaps even to the ports and airfields of embarkation in its homeland—does the cost of intervention expand nearly exponentially? On top of that, the mechanics of moving forces from home bases to the combat zone will become much more difficult. Will other nations provide transit or port rights if it means that their homeland will be subjected to significant attacks? Power-projection nations will find their options limited and will be required to rethink how they project power.

In contrast to the ever more expensive and extremely high technological systems, small, smart, and relatively cheaper drones are creating entirely new challenges across the battlefield. While current Western high technology programmes produce fewer and fewer bespoke weapons systems, the convergence of technological advances is resulting in the proliferation of tens of thousands of cheap, smart systems.

CONCLUSION

The world has entered an era of rapid and converging technological advances in many fields similar to that following WWI. This creates the potential for disruptive shifts by creative applications, especially by combinations of these advances. The key question is whether we will invest in the equivalent of battleships or aircrafts. Will our investments prove to be exquisite and irrelevant or change the face of conflict? Unfortunately, many militaries today are mirroring the navies between the wars. They are applying new technologies in an effort to squeeze another five percent of performance out of older weapons, while under-investing in the evolving technologies that are changing the character of contemporary and future conflicts.

In contrast to the ever more expensive and extremely high technological systems, small, smart, and relatively cheaper drones are creating entirely new challenges across the battlefield. While current Western high technology programmes produce fewer and fewer bespoke weapons systems, the convergence of technological advances is resulting in the proliferation of tens of thousands of cheap, smart systems. Western nations are struggling to find answers to this challenge, and none of them look like the few and bespoke programmes currently consuming the bulk of major procurement programmes.[57]

For small and medium nations, the 'small, smart, and many' represents a great opportunity for their investment programmes. They can generate many of the capabilities of the most expensive current systems at a fraction of the cost. They may also be shifting the balance to the tactical defensive side, which would allow a smaller power to employ effective, affordable A2/AD strategies against a much larger power. They may simply raise the cost of conflict until it is too high for any possible gain.

The critical military functions will remain, but how they will be accomplished will change. Rather than investing everything in few, exquisite and very expensive systems, it makes more sense to explore augmenting them and, in time, replacing them with systems that conform to small, smart, and many.

BIBLIOGRAPHY

"Agricultural UAV Drones Photos – Multi-Spectral Camera," Homeland Surveillance & Electronics LLC, http://www.agricultureuavs.com/photos_multispectral_camera.htm.

Amano, Takashi, "Japan's Micro-Satellites Expand Space Race to Arctic Ice," Bloomberg Business, 16 Jan 2014,http://www.bloomberg.com/news/articles/2014-01-17/japan-s-micro-satellites-expand-space-race-to-arctic-ice-tech.

Amato, Andrew, "Drones at CES 2015 Showcase UAV Technology's Bright Future," Dronelife.com, 14 Jan 2015, http://dronelife.com/2015/01/14/drones-ces-2015-showcase-uav-technologys-bright-future.

Borghino, Dario, "Voxel* paves the way for #D-printed electronics," gizmag, http://www.gizmag.com/voxel8-3d-electronics-printer/35489.

Buchanan, Rose, "3D printer creates jet engine in world first," The Independent, 26 Feb 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/3d-printer-creates-jet-engine-in-world-first-10072740.html.

Condliffe, Jamie, "This is NASA's First 3D-Printed Full-Scale Copper Rocket Engine Part," http://gizmodo.com/this-is-nasas-first-3d-printed-full-scale-copper-rocket-1699394241.

Connor, Will, "Underwater Drones Are Multiplying Fast," Wall Street Journal, 24 Jun 2013, http://www.wsj.com/articles/SB10001424127887324183204578565460623922952.

Department of the Navy FY 2013 Budget Estimates, p. 3.4, http://www.finance.hq.navy.mil/FMB/13pres/FY13_DataBook.pdf.

DeSimone, Joseph, "What if 3D printing was 100x faster?" TED Talks, http://www.ted.com/talks/joe_desimone_what_if_3d_printing_was_25x_faster?language=en.

Erickson, Andrew S., et al., Chinese Mine Warfare: A PLA Navy's 'Assassin's Mace' Capability, Naval War College China Maritime Studies Number 3, p. 14 https://www.usnwc.edu/Research---Gaming/China-Maritime-Studies-Institute/Publications/documents/CMS3_Mine-Warfare.aspx

Farley, Robert, "U.S. Navy Orders 10 Virginia-class Submarines at a Record Cost of $17.6 Billion," The Diplomat, May 3, 2014, http://thediplomat.com/2014/05/us-navy-orders-10-virginia-class-submarines-at-a-record-cost-of-17-6-billion.

Giges, Nancy S., “Top 10 Materials for 3D printing,” ASME.org, https://www.asme.org/engineering-topics/articles/manufacturing-processing/top-10-materials-3d-printing.

“Global Observer High Altitude Long Endurance UAV, United States of America,” airforce-technology.com,http://www.airforce-technology.com/projects/globalobserverunmann.

Golson, Joran, “A Military-Grade Drone That Can Be Printed Anywhere,” wired.com, 16 Sep 2014, http://www.wired.com/2014/09/military-grade-drone-can-printed-anywhere.

Gould, Joe, “US Army 'Dumb' 155mm Rounds Get Smart,” Defense News, 13 Mar 2015, http://www.defensenews.com/story/defense/land/weapons/2015/03/13/orbital-atk-wins-us-army-deal-for-pgk/70222932.

GAO-15-342SP Assessments of Major Weapon Programs, United States Government Accountability Office, March 2015, http://www.gao.gov/assets/670/668986.pdf#page=87.

Koch, Wendy, “Tiny Batteries Could Revolutionize Green Energy,” National Geographic, 16 Nov 2014, http://news.nationalgeographic.com/news/energy/2014/11/141117-nanotechnology-for-better-batteries.

Halverson, Nic, “Drone Missile Kills Electronics, Not People,” Discovery News, 26 Oct 2015, http://news.discovery.com/tech/champ-drone-emp-121026.htm.

“Israel special – IAI’s Harop ups the stakes on SEAD missions,” Flightglobal, Feb 11, 2008, http://www.flightglobal.com/news/articles/israel-special-iai39s-harop-ups-the-stakes-on-sead-221439.

Krassenstein, Eddie, “CloudDDM – Factory with 100 (eventually 1,000) 3D Printers & Just 3 Employees Opens at UPS’s Worldwide Hub,” 3D Printer and 3D Printing News, 4 May 2015, http://3dprint.com/62642/cloudddm-ups.

Krassenstein, Eddie, “Plus-MFg’s +1000k Multi Material Metal 3D printer Shows its Power,” http://3dprint.com/87236/plus-mfg-3d-metal-printer.

Miziolek, Andrzej W, “Nanonenergetics: An Emerging Technology Area of National Importance,” AMPTIAC Quarterly, Vol 6, No 1, Spring 2002, http://ammtiac.alionscience.com/pdf/AMPQ6_1ART06.pdf.

“MK 60 Encapsulated Torpedo (CAPTOR),” http://www.fas.org/man/dod-101/sys/dumb/mk60.htm.

“Nanotechnology Uses of Materials for Multifunctional Capacitors of Future,” iAltEnery.com, http://www.ialtenergy.com/nanotechnology-uses.html.

Naval Air Systems Command: Tomahawk, http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=F4E98B0F-33F5-413B-9FAE-8B8F7C5F0766.

Nicol, Mark, “MoD tests defences against high-street drones as MI5 braces itself for jihadi chemical attack on UK, “Daily Mail, 12 Sep 2015, http://www.dailymail.co.uk/news/article-3232350/MoD-tests-defences-against-high-street-drones-MI5-braces-jihadi-chemical-attack-UK.html.

Osborn, Kris, “Air Force Developing Swarms of Mini-Drones,” Military.com, 27 May 2015, http://defensetech.org/2015/05/27/air-force-developing-swarms-of-mini-drones.

Perry, Tekla S., “Start-up Profile: Skybox Imaging. The satellite-imaging company plans to bring remote sensing to the mass market,“IEEE Spectrum, 1 May 2013, http://spectrum.ieee.org/at-work/innovation/startup-profile-skybox-imaging.

Roggio, Bill, “Troops Find IED Factory in Sadr City,” The Long War Journal, 30 Oct 2008, http://www.longwarjournal.org/archives/2008/10/iraqi_troops_find_ef.php.

Russell, Stuart, et al; “Autonomous Weapons: an Open Letter from AI & Robotics Researchers,” Future of Life Institute, 28 Jul 2015, http://futureoflife.org/open-letter-autonomous-weapons.

Sanborn, James K., “Beacon improves UAV’s cargo-delivery accuracy,” Marine Corps Times, 8 Jul 2012, http://archive.marinecorpstimes.com/article/20120708/NEWS/207080314/Beacon-improves-UAV-s-cargo-delivery-accuracy.

Shalal, Andrea, “Lockheed eyes avatars, 3D printing to lower satellite costs,” Reuters, http://www.reuters.com/article/2014/05/19/us-lockheed-satellites-military-idUSBREA4I00J20140519.

Shapiro, Ari Danial, “Remotely Piloted Underwater Glider Crosses the Atlantic,” IEEE Spectrum, http://spectrum.ieee.org/robotics/industrial-robots/remotely-piloted-underwater-glider-crosses-the-atlantic.

Simonite, Tom, “Project Loon,” MIT Technology Review, http://www.technologyreview.com/featuredstory/534986/project-loon.

Smalley, David, “LOCUST: Autonomous Swarming UAVs fly into the future,” Office of Naval Research http://www.onr.navy.mil/Media-Center/Press-Releases/2015/LOCUST-low-cost-UAV-swarm-ONR.aspx.

Smalley, David, “The Future is Now: Navy’s Autonomous Swarmboats Can Overwhelm Adversaries,” Office of Naval Research http://www.onr.navy.mil/Media-Center/Press-Releases/2014/autonomous-swarm-boat-unmanned-caracas.aspx.

Spector, Ronald, Eagle Against the Sun: The American War with Japan, New York, 1985.

"Switchblade," Aeroenvironment, https://www.avinc.com/downloads/Switchblade_Datasheet_032712.pdf, accessed 3 Sep 2015.

Thompson, Mark, "The Navy's Amazing Ocean-Powered Underwater Drone," Time, 22 Dec 2013, http://swampland.time.com/2013/12/22/navy-underwater-drone.

Thompson, Mark, "The Navy's Amazing Ocean-Powered Underwater Drone," Time, 22 Dec 2013, http://swampland.time.com/2013/12/22/navy-underwater-drone.

"Tiny balls of fire," The Economist, 15 Aug 2015, http://www.economist.com/news/science-and-technology/21660963-nanotechnological-accident-may-lengthen-battery-lives-tiny-balls-fire

Toll, Ian W. Pacific Crucible: War at Sea in the Pacific, 1941-1942, New York, 2012.

Truver, Scott C., "Taking Mines Seriously: Mine Warfare in China's Near Seas," Naval War College Review, Spring 2012, Vol. 65, No. 2, http://www.usnwc.edu/getattachment/19669a3b-6795-406c-8924-106d7a5adb93/Taking-Mines-Seriously--Mine-Warfare-in-China-s-Ne.

"UAV/UCAV – Harpy," Chinese Military Aviation, http://chinese-military-aviation.blogspot.com/p/uav.html4.

Vanian, Jonathan, "Behind the scenes with Facebook's new solar-powered Internet drone and laser technology," Fortune, 30 Jul 2015, http://fortune.com/2015/07/30/facebooks-solar-power-drone-internet-earth.

"US Government makes Aerovel's Flexrotoer ITAR-Free," Aerovel, 24 Nov 2014, http://aerovelco.com/us-government-makes-aerovels-flexrotor-itar-free.

"Vision-based Control and Navigation of Small, Lightweight UAVs," Congress Center, Hamburg, Germany, http://www.seas.upenn.edu/~loiannog/workshopIROS2015uav.

Wenz, John, "Book a Spot Online to Put Your Satellite Into Space," Popular Mechanics, 10 Aug 2015, http://www.popularmechanics.com/space/rockets/news/a16810/heres-the-worlds-first-online-rocket-launch-scheduler.

Whittle, Richard, "Uncle Sam Wants Your Ideas For Stopping Drones: Black Dart Tests," Breaking Defense, 26 Jun 2015, http://breakingdefense.com/2015/06/uncle-sam-wants-your-ideas-for-stopping-drones-black-dart-tests.

Willimex, Alix, "Autonomous Submarine Drones: Cheap, Endless Patrolling," CIMSEC, 5 Jun 2014, http://cimsec.org/autonomous-subarine-drones-cheap-endless-patrolling.

Woollostan, Victoria, "Cheap drones are coming! Researchers successfully build and fly a low-cost 3D printed DISPOSABLE aircraft," Daily Mail, Mar 28, 2014, http://www.dailymail.co.uk/sciencetech/article-2591533/Cheap-3D-printed-drones-coming-Researchers-successfully-build-fly-low-cost-DISPOSABLE-aircraft.html,

ENDNOTES

1. Nancy S. Giges, Top 10 Materials for 3D printing, (*ASME.org*, 2014), https://www.asme.org/engineering-topics/articles/manufacturing-processing/top-10-materials-3d-printing

2. Eddie Krassenstein, CloudDDM – Factory with 100 (eventually 1,000) 3D Printers & Just 3 Employees Opens at UPS's Worldwide Hub, (*3D Printer and 3D Printing News*, 2015), http://3dprint.com/62642/cloudddm-ups/

3. Joseph DeSimone, What if 3D printing was 100x faster?, (*TED Talks*, 2015) http://www.ted.com/talks/joe_desimone_what_if_3d_printing_was_25x_faster?language=en

4. Dario Borghino, "Voxel* paves the way for #D-printed electronics," (*New Atlas*, 2015) http://newatlas.com/voxel8-3d-electronics-printer/35489/

5. Rose Troup Buchanan, 3D printer creates jet engine in world first, (*The Independent*, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/3d-printer-creates-jet-engine-in-world-first-10072740.html

6. Dr. Andrzej W. Miziolek, Nanonenergetics: An Emerging Technology Area of National Importance, (*AMPTIAC Quarterly*, 2002), v._6, n._1, 45. http://ammtiac.alionscience.com/pdf/AMPQ6_1ART06.pdf

7. Wendy Koch, Tiny Batteries Could Revolutionize Green Energy, (*National Geographic*, 2014), http://news.nationalgeographic.com/news/energy/2014/11/141117-nanotechnology-for-better-batteries/

8. Tiny balls of fire, (*The Economist*, 2015), http://www.economist.com/news/science-and-technology/21660963-nanotechnological-accident-may-lengthen-battery-lives-tiny-balls-fire

9. Nanotechnology Uses of Materials for Multifunctional Capacitors of Future, http://www.ialtenergy.com/nanotechnology-uses.html

10. Tekla S. Perry, Start-up Profile: Skybox Imaging. The satellite-imaging company plans to bring remote sensing to the mass market, (*IEEE Spectrum*, 2013), http://spectrum.ieee.org/at-work/innovation/startup-profile-skybox-imaging

11. Book a Spot Online to Put Your Satellite into Space, (*Popular Mechanics*, 2015), http://www.popularmechanics.com/space/rockets/news/a16810/heres-the-worlds-first-online-rocket-launch-scheduler

12. Project Loon, (*MIT Technology Review*), http://www.technologyreview.com/featuredstory/534986/project-loon

13. Global Observer High Altitude Long Endurance UAV, United States of America, (*airforce-technology.com*), http://www.airforce-technology.com/projects/globalobserverunmann

14. Jonathan Vanian, Behind the scenes with Facebook's new solar-powered Internet drone and laser technology, (*Fortune*,2015), http://fortune.com/2015/07/30/facebooks-solar-power-drone-internet-earth

15. James K. Sanborn, Beacon improves UAV's cargo-delivery accuracy, (*Marine Corps Times*, 2012), http://archive.marinecorpstimes.com/article/20120708/NEWS/207080314/Beacon-improves-UAV-s-cargo-delivery-accuracy

16. Vision-based Control and Navigation of Small, Lightweight UAVs, (*Congress Center, Hamburg, Germany*), http://www.seas.upenn.edu/~loiannog/workshopIROS2015uav

Drones at CES 2015 Showcase UAV Technology's Bright Future," (*Dronelife.com*, 2015), http://dronelife.com/2015/01/14/drones-ces-2015-showcase-uav-technologys-bright-future

17. Crop Falcon – UAV for autonomous crop monitoring and operations, (*Youtube*, 2015), https://www.youtube.com/watch?v=m1wyWNhvV8Y

18. Surveillance and tracking of people, (*Youtube*, 2010), https://www.youtube.com/watch?v=tgULkozh32U

19. Agricultural UAV Drones Photos – Multi-Spectral Camera, (*Homeland Surveillance & Electronics LLC*), http://www.agricultureuavs.com/photos_multispectral_camera.htm

20. Autonomous Weapons: an Open Letter from AI & Robotics Researchers, (*Future of Life Institute*, 2015), http://futureoflife.org/AI/open_letter_autonomous_weapons

21. Future Weapons: Explosively Formed Penetrator (EFP), (*Future Weapons TV*, 2011), https://www.youtube.com/watch?v=Pbf7WEVzKcQ

22. Bill Roggio, Troops Find IED Factory in Sadr City, *(The Long War Journal*, 2008), http://www.longwarjournal.org/archives/2008/10/iraqi_troops_find_ef.php

23. Eddie Krassenstein, Plus-MFg's +1000k Multi Material Metal 3D printer Shows its Power, http://3dprint.com/87236/plus-mfg-3d-metal-printer

24. Jamie Condliffe, This is NASA's First 3D-Printed Full-Scale Copper Rocket Engine Part, http://gizmodo.com/this-is-nasas-first-3d-printed-full-scale-copper-rocket-1699394241

25. Kris Osborn, Air Force Developing Swarms of Mini-Drones, (*Military.com*, 2015), http://defensetech.org/2015/05/27/air-force-developing-swarms-of-mini-drones/

26. David Smalley, LOCUST: Autonomous Swarming UAVs fly into the future, (*Office of Naval Research*), http://www.onr.navy.mil/Media-Center/Press-Releases/2015/LOCUST-low-cost-UAV-swarm-ONR.aspx

David Smalley, The Future is Now: Navy's Autonomous Swarmboats Can Overwhelm Adversaries, (*Office of Naval Research*), http://www.onr.navy.mil/Media-Center/Press-Releases/2014/autonomous-swarm-boat-unmanned-caracas.aspx

27. Victoria Woollostan, Cheap drones are coming! Researchers successfully build and fly a low-cost 3D printed DISPOSABLE aircraft, (*Daily Mail*, 2014), http://www.dailymail.co.uk/sciencetech/article-2591533/Cheap-3D-printed-drones-coming-Researchers-successfully-build-fly-low-cost-DISPOSABLE-aircraft.html

28. Jordan Golson, A Military-Grade Drone That Can Be Printed Anywhere," (*wired.com*, 2014), http://www.wired.com/2014/09/military-grade-drone-can-printed-anywhere

29. Ari Danial Shapiro, Remotely Piloted Underwater Glider Crosses the Atlantic, (*IEEE Spectrum*), http://spectrum.ieee.org/robotics/industrial-robots/remotely-piloted-underwater-glider-crosses-the-atlantic

30. Alix Willimex, Autonomous Submarine Drones: Cheap, Endless Patrolling, (*CIMSEC, 2014*), http://cimsec.org/autonomous-subarine-drones-cheap-endless-patrolling/

31. Mark Thompson, The Navy's Amazing Ocean-Powered Underwater Drone, (*Time*, 2013), http://swampland.time.com/2013/12/22/navy-underwater-drone/

32. Fire Ant EFP tank Killer, (*Youtube*), https://www.youtube.com/watch?v=JNboWkzKGkg

33. Central Oregon Off Road Racing, (*XPROHELI*), http://community.xproheli.com/video-gallery

34. UAV/UCAV – Harpy, (*Chinese Military Aviation*),http://chinese-military-aviation.blogspot.com/p/uav.html

35. Israel special – IAI's Harop ups the stakes on SEAD missions, (*Flightglobal*, 2008), http://www.flightglobal.com/news/articles/israel-special-iai39s-harop-ups-the-stakes-on-sead-221439

36. "Switchblade," (*Aeroenvironment*), https://www.avinc.com/downloads/Switchblade_Datasheet_032712.pdf

37. GAO-15-342SP Assessments of Major Weapon Programs, (2015), 79. http://www.gao.gov/assets/670/668986.pdf#page=87,

38. Joe Gould, US Army 'Dumb' 155mm Rounds Get Smart, (*Defense News*, 2015, http://www.defensenews.com/story/defense/land/weapons/2015/03/13/orbital-atk-wins-us-army-deal-for-pgk/70222932/

39. XP2 Quadcopter Off Road Racing Demo Reel - Aerial Video and Photography, (*Youtube*, 2013), https://www.youtube.com/watch?feature=player_embedded&v=QRrSriR5b6s

40. "FPV Racing drone racing star wars style Pod racing are back!, (*Youtube*, 2014), https://www.youtube.com/watch?v=ZwL0t5kPf6E

41. Fire Ant EFP Tank Killer, (*Youtube*, 2009), https://www.youtube.com/watch?v=syuu_g7svoE

42. Mark Thompson, The Navy's Amazing Ocean-Powered Underwater Drone, (*Time*, 2013), http://swampland.time.com/2013/12/22/navy-underwater-drone

43. Autonomous Submarine Drones: Cheap, Endless Patrolling, (*CIMSEC*, 2014), http://cimsec.org/autonomous-subarine-drones-cheap-endless-patrolling

Will Connor, Underwater Drones Are Multiplying Fast, (*Wall Street Journal*, 2013), http://www.wsj.com/articles/SB10001424127887324183204578565460623922952

44. Robert Farley, Ú.S. Navy Orders 10 Virginia-class Submarines at a Record Cost of $17.6 Billion, (*The Diplomat*, 2014), http://thediplomat.com/2014/05/us-navy-orders-10-virginia-class-submarines-at-a-record-cost-of-17-6-billion

45. Andrea Shalal, Lockheed eyes avatars, 3D printing to lower satellite costs, (*Reuters*), http://www.reuters.com/article/2014/05/19/us-lockheed-satellites-military-idUSBREA4I00J20140519

46. Scott C. Truver, Taking Mines Seriously: Mine Warfare in China's Near Seas, (*Naval War College Review*, 2012), v._65, n._ 2, 30. http://www.usnwc.edu/getattachment/19669a3b-6795-406c-8924-106d7a5adb93/Taking-Mines-Seriously--Mine-Warfare-in-China-s-Ne

47. Andrew S. Erickson, et al., Chinese Mine Warfare: A PLA Navy's 'Assassin's Mace' Capability, (*Naval War College China Maritime Studies*), n._3, 14. https://www.usnwc.edu/Research---Gaming/China-Maritime-Studies-Institute/Publications/documents/CMS3_Mine-Warfare.aspx

48. MK 60 Encapsulated Torpedo (*CAPTOR*), http://www.fas.org/man/dod-101/sys/dumb/mk60.htm

49. Scott C. Truver, Taking Mines Seriously: Mine Warfare in China's Near Seas, (*Bibliogov*, 2012), 41.

50. US Government makes Aerovel's Flexrotoer ITAR-Free, (*Aerovel*, 2014), http://aerovelco.com/us-government-makes-aerovels-flexrotor-itar-free

51. Naval Air Systems Command: Tomahawk, http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=F4E98B0F-33F5-413B-9FAE-8B8F7C5F0766

52. DON FY 2013 Budget Estimates, 3-4. http://www.finance.hq.navy.mil/FMB/13pres/FY13_DataBook.pdf

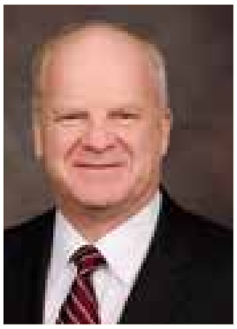
53. Naval Air Systems Command: Tomahawk, http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=F4E98B0F-33F5-413B-9FAE-8B8F7C5F0766

54. Takashi Amano, Japan's Micro-Satellites Expand Space Race to Arctic Ice, (*Bloomberg Business*, 2014), http://www.bloomberg.com/news/articles/2014-01-17/japan-s-micro-satellites-expand-space-race-to-arctic-ice-tech

55. Mark Nicol, MoD tests defences against high-street drones as MI5 braces itself for jihadi chemical attack on UK, (*Daily Mail*, 2015), http://www.dailymail.co.uk/news/article-3232350/MoD-tests-defences-against-high-street-drones-MI5-braces-jihadi-chemical-attack-UK.html

56. Nic Halverson, Drone Missile Kills Electronics, Not People, (*Discovery News*, 2015), http://news.discovery.com/tech/champ-drone-emp-121026.htm

57. Richard Whittle, Uncle Sam Wants Your Ideas For Stopping Drones: Black Dart Tests, (*Breaking Defense*, 2015), http://breakingdefense.com/2015/06/uncle-sam-wants-your-ideas-for-stopping-drones-black-dart-tests/

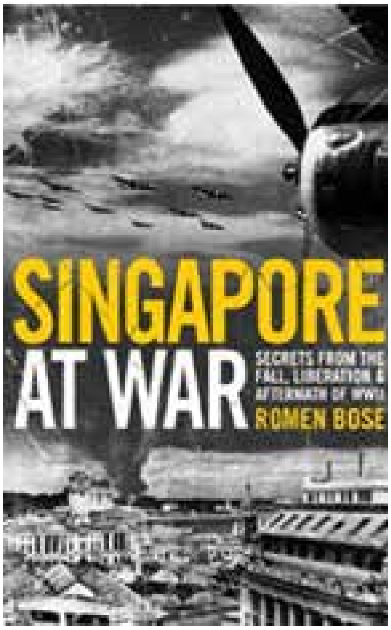


Dr. Thomas X. Hammes has served at all levels in the operating forces in his thirty years in the United States Marine Corps, including commanding an intelligence battalion, an infantry battalion and the Chemical Biological Incident Response Force. He participated in stabilisation operations in Somalia and Iraq and trained insurgents in various places.

Dr. Hammes has a Masters in Historical Research and a Doctorate in Modern History from Oxford University. He is currently a Distinguished Research Fellow at the Institute for National Strategic Studies, National Defense University and an Adjunct Professor at Georgetown University.

He is the author of two books, 16 book chapters, and over 150 articles. He has lectured on the future of conflict, strategy, and insurgency.

Book Review



Romen Bose, *Singapore at War: Secrets From The Fall, Liberations & Aftermath of WWII,* (Singapore, Marshall Cavendish), 2012, 463 pages

By **Joshua Foo**

INTRODUCTION

In a literary genre that consists primarily of military strategies, death of the innocents, and cold hard truths of World War Two (WWII) in Singapore, Romen Bose's three-part volume, *Singapore At War,* falls squarely in the latter category. This may frustrate some readers who, seventy years on, are still struggling to make sense of the mixed bag that caused the suffering of their ancestors.

For the first time, three of Romen Bose's ground-breaking works have been brought together in one volume—providing a panoramic account of Singapore's experience in WWII. These all help to piece the jigsaw of the past in Romen's insightful, tightly focused and fresh analysis of three significant problems in our history.

Romen Bose, born and bred into the world of journalism, begins his career as an intern in the Singapore Press Holdings where he first finds out about the existence of the Battlebox. Since then, he has led teams of reporters in an international news organisation, Agence France-Presse, spearheaded projects in the Singapore Tourism Board and covered analysis on social media at IHS. His repertoire of books written includes research of similar areas—namely WWII and the history of Singapore.[1]

Many of the secrets discussed in the volume *Singapore At War: Secrets From The Fall, Liberations & Aftermath of WWII* were not declassified by various authorities until recent years. These include the highly confidential Battlebox—located nearly 30 feet beneath Fort Canning Hill, the complex was constructed as an emergency bunker for the Combined Operations Headquarters for the Malayan Campaign in the war. The 29-room bunker was fortified with one metre thick reinforced concrete walls to withstand direct hits from bombs and shells. It was fully equipped with a telephone exchange connected to all military and most civilian switchboards in Malaya, including a cipher room for coding and decoding messages.[2]

TARGETED AUDIENCE

Romen Bose's ground-breaking work is targeted at both the casual reader filled with curiosity and also at dedicated research specialists who want to have a good fundamental understanding about the war in Singapore. The Battlebox during the Malayan Campaign is thoroughly discussed in the first volume—*Secrets From The Fall*. In the second part of the volume, *The End Of The War: Singapore's Liberation And The Aftermath Of WWII*, readers explore the few months in 1945 when the war had ended and Britain decided to regain Malaya and Singapore, shedding light into wartime hero Lim Bo Seng. The third and final part of the volume, *Kranji: The Commonwealth War Cemetery and The Politics Of The Dead*, covers the cemetery, discussing how it came about and examines some of those individuals buried there.

The two dominant characters in this memoir by Romen Bose are Bose himself, and arguably Singapore's most important strategist during the war—Lieutenant General Arthur Percival. Bose believes "that the understanding of history is formed on the basis of a disparate collection of facts and details, from differing viewpoints and periods."[3] Though he does not expound on this theology, it is manifest in his unwavering search to uncover the hidden truths of WWII in Singapore and Malaya decades after.

SECRETS OF THE BATTLEBOX

Sealed off and undiscovered until the late 1980s, Bose provides an account of his discovery of the Battlebox when he first began as an intern in the Singapore Press Holdings. As a young and curious journalist, he wandered into the extensively damaged underground headquarters (HQ) together with a fellow photographer. The pictures, appropriately used throughout the book, garner the interest of the readers, similar to how Bose felt whilst first exploring the place. The Battlebox beneath Fort Canning served as the British Command HQ in the last days before the fall. Through the author's research using the archives in the United Kingdom and Asia, he carefully arranged the pieces of the puzzle of what could have happened in the underground nerve centre of the Malayan Campaign.

Drawing on first-hand investigation, accounts of survivors and top-secret documents, the author reveals the fascinating inner workings of the Battlebox. The Battlebox was deemed too small for its intended use even before the war.[4] Lieutenant General Percival, General Officer Commanding (Malaya), constructs another Combined Operations HQ at Sime Road, adjacent to the Royal Air Force HQ. The construction of the new HQ barely finished before the war in Singapore began, in December 1941. Despite the movement of many major operations to the new HQ in Sime Road, the Battlebox was still office to Major General Keith Simmons, responsible for the defence of Singapore's mainland, and other officers from the Navy and Air Force.[5]

This first edition begins with a narrative of 15th February 1942, the day when Lieutenant General Percival signed the inglorious surrender papers in the Ford Motor Factory in Bukit Timah. The hard truths of the day were described in grim detail, casting a dark shadow over the events that happened in Singapore and Malaya over the 70 days of the Campaign.

Bose brings readers back to 8th February, 1942, when Japanese troops crossed the Straits of Johor in a successful landing on the north-west coast of Singapore Island, followed by a second landing near the Kranji River. As communications between personnel at the Sime Road headquarters was poor and layout proven to be impractical, the new headquarters had to be abandoned after the Battle of Kranji.

Details of the campaign unfold as Lieutenant General Percival orders a movement of the Combined Operations Headquarters back to the Battlebox on 11th February, 1942. By the latter stages of the campaign in Singapore, the Japanese were sending aerial attacks on all of Singapore, including Fort Canning which was within range of the Japanese artillery, forcing personnel into the Battlebox. Bose brings readers right down to the site of the Battlebox with his descriptions of how poor living conditions were underground. With 500 officers and men in the Battlebox during that period, conditions were extremely uncomfortable as ventilation systems broke down, causing the underground headquarters to be hot and drowning in the stench of sulphur from the latrines.[6]

One of the most key moments in the Battlebox was the meeting that allowed Lieutenant General Percival to come to a decision to surrender Singapore. Drawing on recently declassified archives, the meeting was held in the Commander, Anti-Aircraft Defence Room on the morning of 15th February, 1942. With senior officers Generals Heath, Simmons and Bennett in attendance, they came to the conclusion that the war could not carry on with the diminishing water supplies, dangerously low fuel reserves and ammunition. As no viable options for launching a counterattack were available, the decision was finally made to surrender to the Japanese.[7]

Bose aimed to let readers understand the history, the use and the final role of the Battlebox in the Malayan Campaign. Throughout the book, it addresses the gap in knowledge on one of the most crucial venues of WWII in Singapore and Malaya, as the secret underground command headquarters in the campaign. To a certain extent, Bose criticises how the military headquarters tried to manage three different things at once, resulting in the failure of managing even one.

THE END OF THE WAR

After the fall of Singapore, effectively losing their 'Impregnable Fortress', the British diverted their attention to the European theatre of war. *The End Of The War: Singapore's Liberation and The Aftermath of WWII* is an account of the ending of WWII in Malaya and Singapore. Using recently-released classified documents, archival photographs and first-hand recollections, insight is given into the string of events and personalities which surrounded British official policy in the Pacific area. The clandestine resistance forces in Malaya and Singapore are also discussed in detail. This book also describes Operation Zipper in Malaya, Operation Tiderace in Singapore as well as the official Surrender ceremony of 12th September, 1945 in Singapore. The final chapter gives readers a good insight of the post-war and anti-colonial social climate. In the appendix of the book are official documents, biographical summaries, bibliography and index.[8]

Operation Zipper—a British plan to capture either Port Swettenham or Port Dickson, Malaya as staging areas for the recapture of Singapore was never fully executed due to the end of the war in the Pacific. Operation Tiderace—the plan to recapture Singapore—was instead put into action following the surrender of Japan. The Allied fleet departed Rangoon on 27th August, 1945, as part of Vice Admiral Harold Walker's force. Sailing for Penang was designated Task Force 11, consisting of the battleship HMS *Nelson* and escort carrier HMS *Attacker*, amongst others. HMS *Nelson* was the flagship of the fleet, and the articles of surrender were signed aboard the battleship on 2nd September, 1945.[9]

But what went on behind the scenes as they prepared to return to the region and, when the Japanese surrendered, to re-establish their authority? After Japan surrendered to the Allies on 15th August, 1945, there was a state of anomaly in Singapore, as the British had not arrived to take control until September. Thousands of Singaporeans lined the streets to cheer the British Military Administration which ruled Singapore between September 1945 and March 1946. However, the failure of the British to defend Singapore had already destroyed their credibility as infallible rulers in the eyes of the locals in Singapore.[10]

The decades after and during the war saw a political awakening amongst the local populace. The rise of nationalist and anti-colonial sentiments was rampant, including a cry for *Merdeka*, roughly translated to 'independence' in the Malay language. The British, on their part, were prepared to embark on a programme of gradually increasing self-governance for Singapore and Malaya.

The majority of this book is part of a build-up of the main plot where every ending leads to a new beginning. Following the surrender of the Japanese in 1945, Singapore's political leaders voiced their demands for independence, determined to move away from British rule.

KRANJI

A picture of serenity today, the war cemetery at Kranji is the final resting place of those who fought and died in the war. In his book, Bose describes that it has been no smooth journey achieving the peace we now see. As much as this book is dedicated to remembering the men and women who gave their lives during the Japanese Occupation, it also covers the struggles faced by the authorities in building a civilian war memorial during the tumultuous period of independence.

The Kranji War Memorial is located at 9 Woodlands Road, in northern Singapore. Dedicated to the men and women from United Kingdom, Australia, Canada, Sri Lanka, India, Malaya, the Netherlands and New Zealand who died defending Singapore and Malaya against the invading Japanese forces during WWII, it comprises the War Graves, the Memorial Walls, the State Cemetery and the Military Graves.[11] The grounds are immaculately maintained by the Commonwealth War Graves Commission, and accessible only from Woodlands Road—the same road that the invading Japanese Imperial Guards Division had marched down on 9th February, 1942.[12]

The War Memorial represents the three branches of the military—the Air Force, Army and Navy. The columns represent the Army, which marches in columns, the cover over the columns is shaped after the wings of a plane, representing the Air Force, and the shape at the top resembles the sail of a submarine, representing the Navy.[13]

Highlighting some of the lesser known facts in the construction of this memorial to British and Commonwealth troops, *Kranji* looks at how the war cemetery in Singapore was built and serves as the first-ever visitor's guide to the cemetery and its environment. The book also underlines some of the more famous residents of the cemetery and their roles in the Malayan Campaign as well as in the Japanese Occupation. Major Ivan Lyon, the famous *Rimau* team and two Victoria Cross winners are examples of persons highlighted by *Kranji*.[14] Bose also expressed his opinions towards the policy against the Japanese War dead and the final entombing of the ashes of the Japanese troops in the Japanese Cemetery along Jalan Chuan Hoe.

Kranji also provides an account of the opening of the Cemetery in 1957 and the creation of a Military Cemetery and finally the Singapore

State cemetery at Kranji. It also delves into the present ceremonies at Kranji and provides a detailed map and layout plan of Kranji and the Japanese cemetery.

CONCLUSION

With three books placed in an exciting and intriguing volume, readers will be able to enjoy this book. This in-depth insight by Bose provides readers with a broad perspective of Singapore's experience in WWII, whilst remaining tightly focused and creative in his attention to detail. The three significant areas of Singapore's military history—namely the Battlebox, the aftermath of WWII and the Kranji War memorial are described in great detail, with good sources of reference, supported with primary and secondary photographic evidence and well balanced with exciting narration as well as facts.

For anyone seeking to learn more about what happened in Singapore during WWII and how it has affected the small nation, *Singapore At War: Secrets From The Fall, Liberations & Aftermath of WWII* is a must-read.

ENDNOTES

[1] Romen Bose Profile, *LinkedIn*, https://uk.linkedin.com/pub/romen-bose/23/74/49a.

[2] Bose, Romen (2005). *Secrets of the Battlebox: The History and Role of Britain's Command HQ in the Malayan Campaign*, Marshall Cavendish Editions (Singapore: Times Publishing Group), 40.

[3] Ibid., Preface.

[4] Ibid., 70.

[5] Ibid., 74.

[6] Ibid., 82.

[7] Ibid., 64.

[8] Ibid., 199.

[9] Ibid., 201.

[10] Ibid., 185.

[11] Kranji War Memorial, *Your Singapore*, http://www.yoursingapore.com/see-do-singapore/history/memorials/kranji-war-memorial.html

[12] Singapore Memorial, *Commonwealth War Graves Commission*, http://www.cwgc.org/find-a-cemetery/cemetery/2053500/SINGAPORE%20MEMORIAL

[13] Kranji War Memorial, *Ghetto Singapore*, http://www.ghettosingapore.com/kranji-war-memorial/

[14] Bose, Romen (2005). *Secrets of the Battlebox: The History and Role of Britain's Command HQ in the Malayan Campaign*, Marshall Cavendish Editions (Singapore: Times Publishing Group), 322.

Richard Marcinko (b. 1940)

by **Delson Ong**

"Change hurts. It makes people insecure, confused, and angry. People want things to be the same as they have always been, because that makes life easier. But, if you are a leader, you cannot let your people hang on to the past."

- Retired US Navy SEAL Commander Richard Marcinko[1]

INTRODUCTION

In the eyes of the public, the United States (US) Navy's Sea, Air and Land Teams, commonly known as the Navy SEALs, are a group of elite individuals that have accomplished incredible feats. Of the many Special Forces teams, one of them is responsible for the death of the founder of Al-Qaeda, Osama bin Laden—SEAL Team Six. Many people would give the credit to SEAL Team Six, but let us not forget the man behind the scenes, the brilliant individual who singlehandedly put together this special team. This person is none other than retired US Navy SEAL commander, Richard Marcinko.

EARLY LIFE

Richard Marcinko was born on 21st November, 1940, in a coal-mining town in Carbon County, Pennsylvania. His parents were immigrants from the Czech Republic, and when he was young, they would mine coal in humid dark tunnels. 'Life was simple, and life was hard,' was how Marcinko described his childhood.[2] Shortly before attending high school, the family moved to New Brunswick, New Jersey, where he attended Admiral Farragut Academy.[3] His parents, however, split up during his high school years, and Marcinko dropped out of high school later that year in 1958.

Feeling that his life could potentially spiral down to meaninglessness, young Marcinko decided to take matters into his own hands. A coincidental encounter with US Marines inspired Marcinko to enlist. His first attempt at enlisting was unsuccessful, as the Marine Recruiter told him to finish high school first before he could apply. But Marcinko did not like that at all. Going back to school was not an option at that point in time. So, a few months later in September, Richard Marcinko tried enlisting with the US Navy. This time round, he was successful.[4]

MILITARY CAREER

After enlistment, Marcinko underwent basic training at the US Navy's Great Lakes facility, before becoming a radioman at a naval base at Quonset Point, Rhode Island, where he worked as a teletype operator as part of a temporary assignment.[5] It was there that he watched a movie—The Frogmen—that determined his career path in the US Navy. He had set his sights on becoming a member of the Underwater Demolition Teams (UDTs); he wanted to be a 'destroyer'.[6]

Underwater Demolition Team

After completing radio school in Norfolk, Virginia, Marcinko applied to join the UDTs, and he arrived at the UDT base at Little Creek, Virginia, on 21st June, 1961. The trainees were told on their first day that should they fail the course, they would have to go back to where they came from. To Marcinko, being sent back to the regular Navy was a pushing alternative, in his estimation.[7] But his chances of graduation from the course were not great, to say the least. Only one out of every five students would make it to graduation day, and Marcinko was determined to make it through. All around him, he watched as hard, experienced men either failed or quit. Knowing that there would not be a second chance, Marcinko worked through fear, physical injuries, harsh verbal abuse, deep ice-cold waters and the ever-present nagging gnaw of fatigue.[8] After months of grueling training, he finally graduated from the course and joined the US Navy's elite UDTs.

Becoming an Officer

Marcinko's outstanding perseverance throughout the course earned him the moniker 'Demolition Dick, Shark Man of the Navy'.[9] Not long after graduation, he was approached by several officers and seniors, who suggested that Marcinko apply for Officer Candidate School. Initially, Marcinko resented the idea, basing it on the fact that it was unlikely for a high school dropout to become an officer; the goal seemed too improbable.[10] However, Marcinko eventually applied and in December 1965, he graduated from Officer Candidate School.

Navy SEALs

Back then, the forerunners of the Navy SEALs were merged in this elite unit, the UDTs. It was only in 1962, when former US President John F. Kennedy realised the need for unconventional warfare, that the SEALs were established. Building on the UDT's elite qualities and water-borne expertise, the SEALs would add land combat skills into their repertoire.[11] Before Marcinko entered UDT, the Navy SEALs were still a part of the elite team (which explained why Marcinko wanted to join the UDT so badly). But the Navy SEALs were separated from the UDT when he graduated from Officer Candidate School, so Marcinko, knowing full well that he wanted to become a SEAL, pulled every string he could to get himself assigned to SEAL Team Two, which he did. After seven years, Marcinko was finally a part of the Navy SEALs.

VIETNAM WAR

Marcinko served two tours in Vietnam from 1967 to 1968, the first of which was located thirteen kilometres west of Tra Noc, South Vietnam. There, Marcinko led his men on a mission to ambush the Vietcong. Despite successfully surprising the enemy, the SEALs faced a well-organised opposition.[12] An intense two hour firefight later, with both sides still locked in battle, Marcinko decided to radio for an air strike—a decision that would secure the victory for Marcinko and his men. But, that decision was not met with praises, as he was criticised by his officers for violating protocol. Going into combat without clearance and calling in an air strike were prerogatives of much more senior officers, not Marcinko himself.[13]

Victory on the battlefield mattered more than anything else to Marcinko, but that was not the case for his commanding officers back at camp. To him, he cared about combat and they cared about careers. To them, Marcinko had threatened the entire chain of command.[14] His insubordination would ultimately lead to the US Navy calling it the 'most successful SEAL operation in the Mekong Delta,' and it was the start of a pattern that would, in time to come, distinguish him from the rest.[15]

First Bronze Star

Marcinko's second Vietnam tour saw him being involved in the Tet Offensive, one of the largest military campaigns of the Vietnam War.[16] Initially tasked with assisting the US Army Special Forces in the urban street fight, Marcinko and his men soon found themselves on another mission—they were tasked to rescue American nurses and schoolteachers who were trapped in hospitals and churches located throughout the city of Châu Dõc, which acted as temporary safe houses until the cavalry arrived. Moving through the once picturesque village, Marcinko led his men from the front, braving machine gun fire and mortar attacks while navigating through the apocalyptic ruin. In the end, he was able to locate the survivors and lead them to safety. Marcinko's bravery under fire during the operation earned him his first Bronze Star.

Post-Vietnam War

After two tours in Vietnam, and a two-year state-side staff assignment, Marcinko was promoted to Lieutenant Commander and assigned the Naval Attaché to Cambodia in 1973, where he led covert operations, amongst many other taskings. Marcinko's ascent up the career ladder meant that he was slowly drifting away from combat. But as luck would have it, he was given a front row seat in the largest foreign policy calamity of the 1970s—the Iranian hostage crisis in 1979.[17]

OPERATION EAGLE CLAW

Operation Eagle Claw was an operation ordered by the US President at that time, Jimmy Carter, to attempt to end the Iranian hostage crisis in Iran's capital city of Tehran. Some fifty-two American diplomats and US Marines were taken hostage on 4th November, 1979 by an armed mob that had surged into the US embassy compound in Tehran.[19]

At that time, Marcinko was one of two Navy representatives for a Joint Chiefs of Staff task force known as the Terrorist Attack Team, and he was in charge of briefing the Chief of Naval operations on intelligence and terrorism.[20] The fact that the hostages, who were diplomats, were tortured indicated that the Iranian government would not settle for a treaty fine print, which prompted Marcinko to participate in the planning of a secret mission (codenamed Operation Eagle Claw) to rescue the hostages. But, despite thorough planning for five months, the mission failed before it even started.

Fortunately, the hostages were freed after 444 days of captivity, ending the Iranian Hostage Crisis. Although the rescue mission was a failure in many ways, it did succeed in one aspect: the failure of Operation Eagle Claw led to the creation of SEAL Team Six.

SEAL TEAM SIX

In the wake of Operation Eagle Claw, founder of SEAL Team Six, Marcinko, was tasked with the design and development of a full-time dedicated counter terrorist team. At that time, the

Navy had only two SEAL teams, and Marcinko deliberately named the new unit SEAL Team Six, in an effort to trick others into thinking that the US had three other SEAL teams that they were unaware of.[21] Under Marcinko, the culture in SEAL Team Six was unlike any other special forces or anti-terrorist team. His men were allowed to grow long hair and wear earrings in order to blend in and maintain covert identities. In addition, every man in Team Six was required to be able to perform every task, no matter how big or small it was. What eventually came out of this unlikely setting set by Marcinko was a unique and hardened group of war fighters who looked like surfers and bikers.[22]

THE BIN LADEN RAID

One of the biggest achievements in SEAL and possibly American history to date would be the execution of Osama bin Laden. Being handpicked to deal with America's number one enemy at the time is a testament to the effective combat capability of the Navy SEALs. However, publicly announcing the heroic deeds of SEAL Team Six was not the best thing after all. The glorification of their victory made them targets as well, and the SEALs knew it. Indeed, a few months later, a SEAL Team Six helicopter was gunned down by a rocket-propelled grenade in Afghanistan. Although it is impossible to say with certainty that naming the executioners led to their deaths, the casual use of the SEAL Teams led to the tragedy, and it only goes to show that the dangers of being a part of this special force are very real.

DECORATED WAR VETERAN

By the end of his military career, Marcinko was a highly decorated war veteran. He was awarded with over a dozen medals. He was awarded four Bronze Stars for his actions during the Vietnam War, and was also a recipient of the Legion of Merit, as well as the Republic of Vietnam Cross of Gallantry with Silver Star, amongst many others.[23]

After retiring from military service, Marcinko authored several books, both fiction and non-fiction. To date, his best book is still his autobiography 'Rogue Warrior'. He continues to serve the community even after his retirement, appearing on talk shows, and will always remain an iconic figure in Navy SEAL history. 🌏

ENDNOTES

1. *Richard Marcinko*, AZ Quotes, http://www.azquotes.com/quote/610084.
2. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 24.
3. *Richard Marcinko*, (Wikipedia) https://en.wikipedia.org/wiki/Richard_Marcinko.

   Why was SEAL 6 Red Cell founder Dick Marcinko jailed?, (Stories of survival, heroism and bravery),http://survivor-story.com/navy-seal-6-red-cell-founder-jailed/.
4. Ibid.
5. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 24. http://www.dickmarcinko.com/bio.aspx
6. Ibid., 24-25.
7. Ibid.
8. Ibid., 26.
9. Ibid., 25.
10. Ibid., 26.
11. https://en.wikipedia.org/wiki/Underwater_Demolition_Team#Birth_of_Navy_SEALs.
12. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 27.
13. Ibid.

14. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 28.

15. Ibid.

    Richard Marcinko, (Wikipedia) https://en.wikipedia.org/wiki/Richard_Marcinko.

16. *Tet Offensive*, (Wikipedia) https://en.wikipedia.org/wiki/Tet_Offensive.

17. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 29.

18. *Operation Eagle Claw*, (Wikipedia) https://en.wikipedia.org/wiki/Operation_Eagle_Claw.

19. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 20.

20. Ibid., 20 & 29.

21. *Richard Marcinko*, (Wikipedia) https://en.wikipedia.org/wiki/Richard_Marcinko.

22. McEwen, Scott and Miniter, Richard, *Eyes on Target: Inside Stories from the Brotherhood of the U.S. Navy SEALs*, (New York, Center Street, 2014), 41-42.

23. *Richard Marcinko*, (Wikipedia) https://en.wikipedia.org/wiki/Richard_Marcinko.

Quotable Quotes

Disasters can overwhelm us if we do not understand our problems and how to reach the right decisions.
– Goh Chok Tong (b. 1941), former Prime Minister and Emeritus Senior Minister of Singapore

Physical fitness is not only one of the most important keys to
a healthy body; it is the basis of dynamic and creative intellectual activity.
- John F. Kennedy (1917-1963), 35th President of the United States

Good character is not formed in a week or a month. It is created little by little,
day by day. Protracted and patient effort is needed to develop good character.
- Gillian Leigh Anderson (b. 1968), American-British film actress, writer and activist

A noble person attracts noble people, and knows how to hold on to them.
- Johann Wolfgang von Goethe (1749-1832), German writer, philosopher and statesman

Find happiness in tribulation, too. Find it in joy alone and
you could lose it, sooner or later, and be left with nothing.
- Siddharth Katragadda (b.1972), Indian-American writer, poet and filmmaker

Most people say that it is the intellect which makes a great scientist. They are wrong: it is character.
- Albert Einstein (1879-1955), German theoretical physicist

If you would take, you must first give. This is the beginning of intelligence.
- Lao Tzu (600-531 BC), Chinese philosopher and founder of Taoism

As people are walking all the time, in the same spot, a path appears.
- Lu Xun (1881-1936), Chinese writer and revolutionist

Champions aren't made in gyms, champions are made from something they have deep inside them —
a desire, a dream, a vision. They have to have last-minute stamina, they have to be a little faster,
they have to have the skill and the will. But the will must be stronger than the skill.
- Muhammad Ali (1942-2016), American boxer and three-time Heavyweight Champion of the World

Darkness cannot drive out darkness: only light can do that. Hate cannot drive out hate: only love can do that.
- Martin Luther King Jr. (1929-1968), American civil rights activist

How we think shows through in how we act. Attitudes are mirrors of the mind. They reflect thinking.
- David Joseph Schwartz (1927-1987), American motivational writer and coach

If you have ideas, you have the main asset you need, and there isn't any limit to what
you can do with your business and your life. Ideas are any man's greatest asset.
- Harvey S. Firestone (1868-1938), American businessman

Chief of Defence Force Essay Competition 2015/2016 Prize Winners

FIRST PRIZE

Finding SAF's Place in the Cyber Age
MAJ Sebestian Xu Jiaheng

SECOND PRIZE

The Value of Sustainability for the SAF
LTA Julie Lim Yee Sin

THIRD PRIZE

Maritime Terrorism Threat in Southeast Asia and the Challenges Faced in Dealing with it
ME6 Joses Yau Meng Wee

MERIT AWARDS

Fact of Science Fiction – Envisioning the Next Technological Disruption in the Present Tense
ME5 Calvin Seah Ser Thong & MAJ Jonathan Quek Choon Keat

Can Singapore Apply Deterrence as an Effective Strategy Against Terrorist Organisations?
ME6 Jerediah Ong

Beyond the Fourth Generation – A Primer on the Possible Dimensions of Fifth Generation Warfare
LTC Victor Chen Kanghao

Is Deterrence an Archaic Concept or a Relevant Strategy?
CPT Jamie Lee Wen Jie

Engineering our Future – Forging the SAF's Leading Edge
ME5 Wong Chong Wai

Bridging the Gap for Hybrid Warfare
LTC Ingkiriwang Shawn

Trajectory of National Service: Revisiting the Past, Evaluating the Present and Ponder for the Future
CPT Lee Zi Yang

The Hammer and the Swiss Army Knife: Hybrid Warfare and its Implications for Singapore and the SAF
MAJ Edwin Chua, LTA Joseph Lee & LTA Brandon Tan

COMMENDATION AWARDS

Beyond SAF50: Maintaining the SAF's Edge amidst Global, Regional, and Domestic Challenges
CPT James Yong Dun Jie

Hybrid Warfare – A Low-Cost, High-Return Threat to Singapore as a Maritime Nation
MAJ Bertram Ang Chun Hou

Man of the Machine
LTA(NS) Chin Hui Han, Ms Annalyn Ng & Ms Sonya Chan

China's agreement to the Code for Unplanned Encounters at Sea (CUES):
The significance for maritime security and stability in the Indo-Pacific.
LTC Eng Cheng Heng

Can Deterrence Work for Small Nations?
MAJ Leong Tyng Wey

Lessons from the Use of Low-Level Aerial Photography in
Imagery during the Cuban Missile Crisis of 1962
CPT Lim Guang He

Unmanned Aerial Vehicles – A Clear and Present Danger, and What we can do about Them
CPT Jerry Chua

Winning Hearts through Communication –
A Social Media Engagement Strategy for the Military
MAJ Tan Kok Yew

South China Sea – Security implications to Southeast Asia due to China's
Aggressive Actions in Spratly and Paracels Islands and US Naval Deployment into South China Sea
LTA Regina Tan Yun Pei

The Economic Impact on the Global Security Landscape
ME4 Gerald Goh Qi Wen

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

pointer

Vol. 42 No. 4 [2016]

THE JOURNAL OF THE SINGAPORE ARMED FORCES

ISSN 2017-3956