

---

P O  N T E R

---

JOURNAL OF THE SAF

VOL.48 NO.1  
[2022]



# Editorial Board

---

## Advisor

**BG Tan Tiong Keat**

## Chairman

**COL Paul Cheak Seck Fai**

## Deputy Chairman

**COL(NS) Irvin Lim Fang Jau**

## Members

**COL(NS) Tan Swee Bock**

**COL(NS) Benedict Ang Kheng Leong**

**COL(NS) Victor Huang**

**COL Koi Eng Chew**

**COL Kenneth Gn**

**COL Ong Jack Sen**

**ME6 Leong Hoe Meng**

**MAJ(NS) Charles Phua Chao Rong, PhD**

**Ms Christina Kwok**

**Mr Desmond Loo**

**Mr Eddie Lim**

**Mr Daryl Lee Chin Siong**

**Mr Eugene Chew**

**Ms Sonya Chan**

**Mr Chin Hui Han**

**CWO Chua Hock Guan**

**Professor Pascal Vennesson**

**Dr Chang Jun Yan**

## Editorial Team

### Editor

**Ms Helen Cheng**

### Assistant Editor

**Mr Bille Tan**

### Research Specialists

**CPL Ng Man Chiu Enrique**


**CPL Deng Chen Hao**

**PTE Shin Min Seo**

**PTE Joel Yuen Zheng Wei**

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

# C CONTENTS



## iii Editorial

- 1 Non – Offensive Defence As a Strategy for National Security  
By **LTC Phang Chun Chieh**
- 12 The Centre of Gravity Concept in Clausewitz’s ‘On War’  
By **MAJ Edward Khoo Chun Kiat**
- 21 Can a Small State Challenge a Much Larger State or A Collection of Enemy States?  
By **ME5 Lim Sher Hern**
- 32 Cyber Power — An Experimental Framework  
By **MAJ Alex Hoh Li Wei**
- 44 Applying the Jus Ad Bellum Framework to Cyberspace  
By **LTA(NS) John Yap & LTA(NS) Ryan Lee**

# Editorial

POINTER Vol 48, No. 1 is a compilation of essays from students of our local Command and Staff Course (CSC) of the Goh Keng Swee Command and Staff College (GKS CSC) as well as from two National Servicemen.

The first of the essays, 'Non-Offensive Defence As A Strategy For National Defence' is written by LTC Phang Chun Chieh. In this essay, LTC Phang argues that, against conventional state-based threats, Non Offensive Defence (NOD) is a viable national security strategy if the state has a defensible geography, a benign geopolitical neighbourhood, and low geostrategic value. Against terror, LTC Phang argues that the stove-piped nature of military NOD has limited effectiveness and that it is useful only as part of a larger umbrella of counterterrorism (CT) strategies. He first discusses the concept of conventional NOD and illustrates its permissive conditions using New Zealand and Singapore as examples, before presenting the applications and limitations of NOD as a CT strategy.

MAJ Edward Khoo Chun Kiat wrote the next essay, 'The Centre Of Gravity Concept in Clausewitz's *On War*'. In this essay, MAJ Khoo seeks to illustrate that even though the concept of centre of gravity (COG) may be abstract, it can still be of use to military planners. He highlighted various problems with the concept such as subjectivity and mistranslation which could lead to confusion and a lack of utility. An example of this he adds, is the lack of a common definition of the COG, as well as the different conclusions which can be derived from the multitude of conflicting methodologies that have arisen even in the same scenario. However, MAJ Khoo also explains that the COG can still be a useful concept as it helps planners understand increasingly complex operating environments by revealing relations within the multiple systems, distinguishing between the important and the peripheral. He feels therefore, that the COG enables planners to focus actions on what are important and enhances efficiency.

The third essay, 'Can A Small State Challenge A Much Larger State Or A Collection Of Enemy States?' is written by ME5 Lim Sher Hern. Here, ME5 Lim discusses how, despite the odds stacked against them, small states can still employ an effective conventional

deterrence strategy. He first examines the concept of deterrence before exploring the issue of deterrence through military superiority. He then analyses other approaches to deterrence, such as total defence and alliance. ME5 Lim also highlights that it is in the interests of small states to pursue some form of deterrence against potential adversaries because an armed conflict can threaten their very existence. However, he concludes that deterrence is not a permanent solution to security problems. It is a dynamic posture that has to be maintained to ensure that the state does not pay a heavy price for the devastation of war. In his opinion, successful deterrence is simply an extension of time to address the underlying geopolitical issues.

In the following essay, 'Cyber Power – An Experimental Framework', MAJ Alex Hoh Li Wei highlights that Cyber is the fifth domain after Air, Land, Sea and Space. In his opinion, cyber is evolving and contested by economic, security and civil interests. He stresses that dynamism in cyber must be matched with dexterity in policy and decision-making. However, many leaders remained unfamiliar with this domain. Consequently, responses may fail to address root-causes, exacerbate volatility, generating unexpected emergences in the complex and interconnected cyber domain. In this essay, MAJ Hoh suggests a framework for cyber power. He exemplifies the application of this framework to operationalise threat-intelligence. He then explores gaps across issues relating to threat appreciation in cyberspace. Changes happen daily in the cyber domain and the framework is not definitive.

LTA(NS) John Yap and LTA(NS) Ryan Lee wrote the final essay, 'Applying The Jus Ad Bellum Framework To Cyberspace'. In this essay, LTA(NS) Yap & LTA(NS) Lee outline and explore the challenges involved in the application of the *jus ad bellum* framework to cyberspace. In the essay, the authors sought to address three central issues. First, how norms of international law developed in a pre-cyber age, govern cyberspace. Then, they examined when cyber operations would rise to the level of cyber warfare. Thirdly, they explored when cyber operations would trigger the victim state's right to self-defence and what problems would impede the exercise of that right.

# NON-OFFENSIVE DEFENCE AS A STRATEGY FOR NATIONAL SECURITY

By: LTC Phang Chun Chieh

## ABSTRACT

In this essay, the author argues that, against conventional state-based threats, Non Offensive Defence (NOD) is a viable national security strategy if the state has defensible geography, a benign geopolitical neighbourhood, and low geostrategic value. Against terror, the author argues that the stove-piped nature of military NOD has limited effectiveness and that it is useful only as part of a larger umbrella of counterterrorism (CT) strategies. He first discuss the concept of conventional NOD and illustrate its permissive conditions using New Zealand and Singapore as examples, before presenting the applications and limitations of NOD as a CT strategy.

*Keywords: Security; Terrorism; Deterrence; Applications and Limitations; Non-Offensive Defence*

## INTRODUCTION

Introduced at the height of the Cold War, non-offensive defence (NOD) provided an 'alternative defence' concept to NATO's Follow-on Forces Attack and nuclear deterrence strategies against the Warsaw Pact.<sup>1</sup> NOD seeks to minimize bellicose and escalatory interstate relations in an anarchic and 'self- helping' international system, by shifting the offense-defence balance towards defence and non-provocation.<sup>2</sup> It helps reduce the security dilemma while maintaining a credible deterrence against aggression. Critics, however, argue that NOD is utopian and that it wrongly assumes a hegemonic attacker could be sufficiently deterred, or repulsed, into accepting the geopolitical status quo ante.<sup>3</sup>

Post-Cold War, the global security environment has become more volatile, uncertain, complex, and ambiguous (VUCA). On top of conventional threats, national security interests have deepened and broadened to include, amongst others, non-conventional threats such as terrorism and its societal impact. After 18 years of the global war against terror post-9/11, however, a decisive victory remains elusive. Based on a Brown University study, the war has cost over \$6.4 trillion and 801,000 lives.<sup>4</sup> Yet, terrorism has not abated but has become more pervasive. Therefore, given the new security environment, I will devote some attention to explore NOD as a possible alternative to the offensive approach against terror, while maintaining

the primacy of analyzing the viability of NOD from a conventional angle.

The author argues that, against conventional state-based threats, NOD is a viable national security strategy if the state has defensible geography, a benign geopolitical neighbourhood, and low geostrategic value. Against terror, I contend that the stove-piped nature of military NOD has limited effectiveness and that it is useful only as part of a larger umbrella of counterterrorism (CT) strategies. I will first discuss the concept of conventional NOD and illustrate its permissive conditions using New Zealand and Singapore as examples, before presenting the applications and limitations of NOD as a CT strategy.

## CONCEPT OF CONVENTIONAL NOD

A state which cannot ascertain if the military preparations of another are for defensive or offensive purposes would experience a security dilemma.<sup>5</sup> It may then adopt matching countermeasures to increase its security, which in turn could be perceived as threatening to others. This perpetuates a cycle of insecurity that could trigger an arms race and worsen interstate tensions, thereby encouraging conditions for escalation and war. NOD's value proposition, therefore, is that states can mutually avoid the security dilemma if they adopt a defensive strategic posture that

provides credible defence without threatening others. According to Møller & Wiberg, NOD seeks to: (1) facilitate arms control and disarmament by removing insecurities due to competitive arms dynamics; (2) enhance peace by eliminating the need for pre-emptive and preventive wars; and (3) provide effective yet non-suicidal defence options.<sup>6</sup>

Barnaby & Boeker comprehensively defined NOD as: 'The size, weapons, training, logistics, doctrine, operational manuals, war-games, maneuvers, textbooks used in military academies, etc. of the armed forces are such that they are seen in their totality to be capable of a credible defence without any reliance on the use of nuclear weapons, yet incapable of offence.'<sup>7</sup> That one is perceived to pose no threat is important. Whether a state's NOD strategy would be interpreted as such by others depends on how aligned its national policy and military doctrine are to the principle of non-offense. National policy goals dictate military doctrine, which determines force structure and equipment requirements. The latter are rarely unambiguously defensive or offensive. Special Forces can be deployed in CT homeland defence or covert insertion operations. An amphibious ship may be used for humanitarian or power projection purposes. A state's non-offensive claim is credible only if its policy goals are clearly peaceful and manifest as defensive military doctrine. This alignment can be further strengthened through various NOD approaches, such as 'defensive defence', 'non-provocative defence', 'confidence-building defence', and 'structural inability to attack'.<sup>8</sup>

## CONDITIONS THAT MAKE NOD A VIABLE NATIONAL SECURITY STRATEGY

In employing NOD as a national security strategy, a state ultimately seeks to ensure its sovereignty by managing the threat perception between itself and other states. However, can any state adopt a NOD strategy in our realist world? Simply being perceived as non-offensive or defensive is an insufficient and somewhat subjective guarantee of national security. An adequate security policy should also consider and address the strategic environment that it would operate within. For NOD to be a viable national security strategy, states must satisfy the three key strategic conditions of (1) defensible geography, (2) benign geopolitical environment, and (3) low

geostrategic importance. These conditions make the state not only feel more secure and hence be less aggressive in their defence outlook, but also appear less vulnerable to aggression by others.

## Defensible Geography

Territorial integrity is key to state sovereignty. To advance an offensive, attackers must gain territory and hold ground. Physical terrain, therefore, forms a natural first layer of defence. Borders such as mountain ranges and expansive water bodies are more defensible and less easily breached than those that are flat, porous, and accessible. Additionally, strategic depth, in terms of a vast internal territory and a resource-filled hinterland, allows defenders to reconstitute and sustain their forces further inland, thin-out invading troops, and launch counter-offensives to repel attackers out of the state. States that possess these terrains are thus more secure and less likely to be successfully invaded. For example, Switzerland is surrounded by alpine borders and has rarely been invaded, while Russia leveraged its strategic depth to defend itself and defeat Napoleon's and Hitler's invading troops.<sup>9</sup> Conversely, Kuwait, a small state which shares a long, porous border with Iraq, was defenceless against its more powerful neighbour.

A state's human geography, specifically its population make-up, is another factor that adds to its geographical defensibility. It is easier to rouse nationalistic sentiments and strengthen national unity in an ideologically and ethnically homogenous population. Such unity would allow the state to mobilize popular resistance to fight a guerrilla-like people's war in self-defence, thereby making an invasion more costly for the belligerent. For example, Mao's 'active defence' and 'people's war' strategies reflect the Chinese Communist Party's intent to mobilize and militarize its nationalistic society to liberate itself against aggressors.<sup>10</sup> Therefore, for a state blessed with defensible terrain and popular nationalistic support, a NOD strategy premised on deterrence by denial is achievable.

## Benign Geopolitical Environment

Two intricately linked factors affect a state's interpretation of its geopolitical environment, which in turn determines its security approach. First, past experiences, such as occupation by foreign powers and

conflict, deepen the 'sense of threat' and shapes its strategic culture and security outlook today.<sup>11</sup> Second, a hostile regional environment characterised by interstate tensions and identity politics such as populist nationalism would dictate that a state adopts a more aggressive posture to deter attacks by punishment.<sup>12</sup> States that experience historical and present animosity with its neighbours would find themselves hard-pressed to employ a non-offensive national security strategy. Israel is a good example. Including its war for independence, Israel has fought eight wars with its Arab neighbours since the 1940s.<sup>13</sup> Given its additional lack of strategic depth and porous borders, it must maintain a strong military for pre-emptive and preventive wars and cannot afford to adopt a NOD posture in its geopolitically hostile neighbourhood.<sup>14</sup>

**A hostile regional environment characterised by interstate tensions and identity politics such as populist nationalism would dictate that a state adopts a more aggressive posture to deter attacks by punishment.**

However, NOD strategies are viable if the regional geopolitical environment promotes peace, mutual trust and cooperation, and a rules-based order between states. In the case of Switzerland, a foreign policy of neutrality officialized at the 1815 Vienna Congress sought to unilaterally assure others of its geopolitical and military intent. This has proven to be effective when coupled with other conditions such as credible defence and defensible geography, as Switzerland has not been invaded since the policy's implementation.

Transparency of intent, therefore, helps to allay security concerns and lays the foundation on which states can build trust and gain confidence with each other. After centuries of infighting culminating in the World Wars, Europe has also turned its back on a violent past. Its states have embraced political and economic cooperation mechanisms within the European Union and global system to meet their national interests, rather than resort to arms. This led to a more benign intra-continental security environment that has

facilitated the adoption of more defensive strategies amongst its states.

## Low Geostrategic Importance

In a world dominated by maritime trade and energy flows, a global power must ensure its unfettered access to its worldwide commerce and energy supplies. States that border maritime chokepoints, control critical sea lines of communication (SLOC), or possess vast energy reserves of oil or natural gas are, therefore, strategically important to such powers.<sup>15</sup> Their value makes them more vulnerable to strategic contention between competing powers, which may compel these states to choose sides. Covetous neighbours may also turn aggressive and contest or even invade and take over energy-rich territories. The Middle East possesses several examples, such as the United Arab Emirates (UAE) and Kuwait. The UAE border the Strait of Hormuz chokepoint, a vital oil artery through which 30% of seaborne oil passes through.<sup>16</sup> At the Western end of the Persian Gulf, Kuwait's access to oil prompted an invasion from neighbouring Iraq beset with debt.<sup>17</sup> Given the security vulnerabilities that come with their geostrategic value, these states would have to maintain stronger militaries that can inflict punishment and deter potential aggressors.

The author examines two examples—New Zealand (NZ) and Singapore—to illustrate why states can consider NOD as a viable national security strategy only if the three permissive conditions described above are fulfilled.

## NOD IS VIABLE FOR NEW ZEALAND...

### Defensible Geography

NZ is remotely located at least 1,500 kilometers from its nearest neighbour Australia, with whom it shares a close relationship. The South Pacific Ocean, therefore, serves as a vast aquatic defensive buffer against offensive advances from any direction. Given its land size (268,000km<sup>2</sup>) which supports a small population (4,700,000), and an abundance of mountains, lakes, and arable land, NZ also enjoys the strategic depth for subsistence and the sustenance of defensive operations. Moreover, NZ citizens are fiercely protective of their national identity and are known to be united and resilient, thereby adding to the state's social defence against adversity and attacks.<sup>18</sup>

## Benign Geopolitical Environment

Since it became a British colony, NZ's sovereignty has never been threatened, except during a brief eight-month period in 1942 when it had to prepare against a Japanese Navy that held command of the Pacific.<sup>19</sup> According to its latest Defence White Paper and Defence Policy Statement, NZ will not 'face a direct military threat in the foreseeable future.'<sup>20</sup> It enjoys excellent political, military, economic, and social and cultural relations with Australia. Importantly, both countries also share common security interests and pledge mutual support when one is faced with a security threat. With its South Pacific island neighbours, NZ maintains strong Maori cultural and historical ties which underpin peaceful relations.



*The current NZ Army Multi-terrain Camouflage Uniform (MCU), in service since 2013.*

## Low Geostrategic Value

As an island nation at the southwest edge of the Pacific Ocean, NZ does not border or control any maritime chokepoints or critical SLOCs. It also does not possess abundant reserves of energy, with dairy products listed as its most valuable export.<sup>21</sup>

NOD strategies, therefore, are viable for NZ as it is unlikely to face conventional threats. NZ's small military of only 14,900 personnel (or 0.3% of the population), including reserves and civilians, is sufficient for its largely non-offensive roles.<sup>22</sup> These tasks include defending key physical and electronic lines of communication, ensuring co-operative security of the Southern Pacific, fulfilling obligations to defence treaties and arrangements, for e.g. the Five Power Defence Arrangement, and contributing internationally in humanitarian and peacekeeping missions. Its Air Force focuses on maritime surveillance and airlift and

lacks fighter and assault capabilities. Its Navy, meanwhile, operates only two frigates, one amphibious ship, one replenishment tanker, and a small number of littoral patrol crafts to secure its vast maritime environment. In the absence of conventional threats, NZ can still meet its security interests with a NOD strategy and maintain a small military without having to worry about matching its force capabilities with other states.

## ... BUT NOT FOR SINGAPORE

### Geographically Indefensible

Singapore is a small island state sandwiched between peninsular Malaysia and the Indonesian Riau archipelago. The narrow Johor Strait between Singapore and Malaysia is an ineffective northern barrier against invasion. In fact, during World War II (WWII), Japanese forces crossed the Johor Strait to invade Singapore even after the main Causeway link-bridge between both states was destroyed. To the south, while the Singapore Strait (SS) provides around 19km of separation from Indonesia, it remains an ineffective buffer against long-range artillery attacks. It is densely populated with 5,700,000 people on 724km<sup>2</sup> of land, has no resource hinterland, and thus has no strategic depth to fend off attacks. Adversaries may also weaken Singapore's national unity and resilience against attacks by triggering dormant racial or rich-poor fault lines in its pluralistic society.

### Vulnerable in a Volatile Neighbourhood

Historical experiences have entrenched a sense of insecurity within Singapore's political elites. Singapore's fall to the Japanese in WWII highlighted the need for an independent and robust national defence against aggressors. Communist influence through the Malayan Communist Party threatened to undermine state sovereignty. Indonesia's low-intensity Konfrontasi attacks in Singapore, the deadliest of which was on the MacDonald House bombing, showed that neighbours were open to violent sabotage and subversion.<sup>23</sup> Recent relations with neighbours have become more cordial and co-operative. Yet, tensions continue to simmer beneath a calm surface. With Malaysia, issues that affect Singapore's vital interests, such as disagreements

over bilateral water agreements and maritime territorial disputes, resurface regularly.<sup>24</sup> With Indonesia, its 'big brother' mindset towards Singapore often results in insensitive behaviour, such as labelling Singapore as a 'Little Red Dot' and a 'small country'.<sup>25</sup> These issues typically coincide with the neighbours' election cycles, thereby strengthening claims that others use Singapore as a 'bogeyman' for political distraction.<sup>26</sup>



*MacDonald House, Orchard Road, Singapore.*

## Geo-Strategically Important

Singapore's location allows it to monitor and control maritime traffic entering and leaving the Straits of Malacca and Singapore (SOMS). SOMS is the world's second-busiest waterway for trade, oil, and gas shipping, and it is of strategic interest to the US and China, two global powers and top energy importers.<sup>27</sup> As a maritime nation, Singapore would also be concerned with its maritime trade's secure and free access through its neighbours' waters, for its economic prosperity and survival.<sup>28</sup>

**The Straits of Malacca and Singapore is the world's second-busiest waterway for trade, oil, and gas shipping, and it is of strategic interest to the US and China, two global powers and top energy importers.**

Given these unconducive strategic conditions, it would be unfeasible for Singapore to adopt NOD as its national security strategy. Instead, to secure its national interests, it must deter by punishment. In a conflict scenario, Singapore must prevent its SLOCs from being disrupted, and thus cannot merely rely on defensive measures within its borders. The heightened sense of vulnerability is reflected in the Singapore Armed Forces' (SAF) doctrine of forward defence and pre-emption.<sup>29</sup> It aims to overcome Singapore's lack of strategic depth through the ability to project power further afield to: (1) secure its SLOCs, (2) bring the fight away from its economic homeland, and; (3) strike first in self-defence. This doctrine is operationalised through assets such as the High Mobility Artillery Rocket System (HIMARS) artillery, fighter and refueling tanker aircrafts, submarines, strike-capable ships, and amphibious landing ship tanks.

## NOD AGAINST TERROR?

Having covered NOD's applicability for conventional security, the author now shifts the discussion towards the feasibility of NOD against terrorist threats in today's new security environment. To what extent has the increasingly costly offensive against terrorists deterred them? Will a NOD strategy that maintains credible military deterrence against aggression, but poses no threat to the terrorist, work better instead? The author contends that, like its offensive counterpart, the stove-piped nature of military NOD has its limitations, and that it is useful only as part of a larger umbrella of CT strategies.

## Applying Military NOD to CT

How does one use the blunt military instrument non-offensively against terrorists? The author feels that the most effective way would be to leverage the military's security training and resources and deploy them in preventive CT operations to harden targets, protect key installations (KINS), and control borders. Target hardening would make important people, for e.g. government officials, places, and signature events like The Shangri-La Dialogue, difficult to attack. Protection of KINS would secure critical infrastructure such as transportation hubs,

telecommunication centres, banks and power stations. Border control involves surveillance and patrol of air, land, and sea borders to detect and prevent the smuggling and intrusion of terrorists and their equipment.<sup>30</sup> One should also note that while the military is most suitable for these security tasks, it does not execute them alone but leverages intelligence sharing and support from other security agencies, for e.g. police and customs, as well.



*The scene of the October 2012 Aleppo bombings, for which al-Nusra Front claimed responsibility.*

## Limitations

However, a military NOD strategy in the form of preventive CT is a stove-piped approach to a broader security issue. First, prevention is not absolute. It is impossible to completely prevent a terrorist incident. Against states, it is easier to predict and counter enemy attacks on conventional military targets. For terrorists, however, anything can potentially be a target, especially if their intent is to attrite social resilience on their terms. Second, NOD as a CT strategy, wrongly assumes that all terrorists are rational actors who can be deterred by denial. A determined terrorist organisation can see the continued struggle and violence against the state and society as an avenue to rouse support for their cause. Additionally, suicide bombers who are motivated by radical ideology, or, threats or rewards to their families, can be too desperate to be deterred. Third and most importantly, NOD as a military solution is insufficient. The fight against terrorism is a battle of both arms and ideas.<sup>31</sup>

The state must employ other non-military instruments to: (1) block terrorist ideology from spreading, (2) moderate extremist views, (3) rehabilitate captured terrorists and reintegrate them to society, (4) eradicate their financial sources, and; (5) resolve disputes and societal conditions that germinate extremism.<sup>32</sup> Ultimately, the fight against terrorism is not a military campaign, but a 'contest for the hearts and minds of ordinary Muslims around the world.'<sup>33</sup> NOD simply makes up one end of the military spectrum amongst a broader umbrella of non-military options that a state must leverage to maximise its chances of success against terrorism.

**The fight against terrorism is a battle of both arms and ideas.**

## CONCLUSION

Even as our world becomes more globalised with more avenues for diplomatic and peaceful resolution of interstate differences, geopolitics remain inherently realist and pragmatic. As such, NOD as a national security strategy against conventional threats is only viable for states that are: (1) geographically defensible, (2) not threatened by the regional strategic environment, and (3) of low strategic value in the international order. With the deepening and broadening of national security interests post-Cold War, states also face more non-conventional security threats, such as terrorism. These threats typically carry ideological undercurrents beneath their violent surfaces. Therefore, even less antagonistic military strategies such as NOD are ineffective if employed alone to combat terror. NOD is only viable as a CT strategy if used in tandem with other non-military options that address the ideological aspects.

## BIBLIOGRAPHY

- Barnaby, F., & Boeker, E. (1988). Non-nuclear, non-provocative defence for Europe. In P.T. Hopmann & F. Barnaby (Eds.), *Rethinking the nuclear weapons dilemma in Europe*. New York: St. Martin's Press.
- Butfoy, A. (1997). Offence-defence theory and the security dilemma: The problem with marginalizing the context. *Contemporary Security Policy*, 18(3), 38- 58. <https://doi.org/10.1080/13523269708404168>
- Chua, D. W. B. (2015, March 16). Konfrontasi: "Why it still matters to Singapore. RSIS Commentary 0 j4\_ <https://www.rsis.edu.2s/wp-content/uploads/2015/03/COI5054.pdf>
- Collins, J. M. (1998). *Military geography for professionals and the public*. Washington D.C: University of Nebraska Press
- Crawford, N.C. (2019, November 13). United States budgetary costs and obligations of post- 9/11 wars through FY2020: \$6.4 trillion. 20 years of war: A cost of war research series. Accessed 20 April 2020 from <https://wat.son.browne.du/costsofwarfiles/cow/imcelpapers/2019/US%20Budgetary%20Costs%20of%20Wars%20November%202019.pdf>
- Crawford, N.C., & Lutz, C. (2019, November 13). Human cost of post-9/11 wars. 20 years of war: A cost of war research series. Accessed 20 April 2020 from <https://wat.son.browne.du/costsofwarfiles/cow/imcelpapers/2019/Direct%20War%20Deaths%20COW%20Estimate%20November%202013%202019%20FINAL.pdf>
- Crelinsten, R. (2014). Perspectives on counterterrorism: From stovepipe to a comprehensive approach. *Perspectives on Terrorism*, 8(1), 2- 15.
- Desker, B. (2015, October 14). Challenging times in Singapore-Indonesia relations. RSIS Commentary 216. <https://www.rsis.edu.s2/wp-content/uploads/2015110/COI5216.pdf>
- Fischer, D., & Bloomgarden, A. (1989). Non-offensive defense. *Peace Review*, 1(2), 7- 11. <https://doi.org/10.1080/10402658908425489>
- Flanagan, S. (1988). Nonoffensive defense is overrated. *Bulletin of the Atomic Scientists: Nonoffensive Defense*, 44 (7), 46-48. <https://doi.org/10.1080/00963402.1988.11456201>
- Fukuyama, F. (2006, February 19). After neoconservatism. *The New York Times*. Accessed on 20 April 2020 from <https://www.nytimes.com/2006/0219/maezinelafter-neoconservatism.html>
- Global Commission. (2019). *A new world: The geopolitics of energy transformation*. Accessed 20 April 2020 from [https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Jan/Global\\_commission\\_geopolitics\\_new\\_world\\_2019.pdf](https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Jan/Global_commission_geopolitics_new_world_2019.pdf)
- Huang, A. C. (2001). Transformation and refinement of Chinese military doctrine: Reflection and critique on the PLA's view. In J. Mulvenon & N. D. Yang (Eds.), *Seeking truth from facts: A retrospective on Chinese military studies in the post-Mao era*. Santa Monica, CA: RAND Corporation. <https://www.rand.org/content/dam/rand/pubs/conf/proceedings/CF160/CF160.ch6.pdf>
- Israel MFA. (n.d.) Israel's wars. Israel Ministry of Foreign Affairs. Accessed 20 April 2020 from <https://mfa.gov.il/MFA/AboutIsrael/History/Pages/Israel-\\Wars.aspx>

Jaipragas,B. (2018, December 5). Cross borders: Malaysia and Singapore continue to dispute air and sea boundaries. South China :Morning Post. Accessed 20 April 2020 from <https://www.scmp.com/news/asia/southeast-asia/article/2176552/cross-borders-malaysia-and-singapore-continue-dispute-air>

Lawson, F. H. (2001). Rethinking the Iraqi Invasion of Kuwait. *Review of International Affairs*, 1(1), 1-20

Leighton, M., & Rudney, R. (1991). Non-offensive defense - Toward a Soviet-German security partnership. *Orbis-A Journal of World Affairs*, 35(3), 377- 393.

MICA. (2003). Water Talks - If only it could Singapore: Ministry of Information, Communications and the Arts Singapore

Ministry of Defence, New Zealand. (2016). Defence white paper. Accessed 20 April 2020 from <https://www.defence.govt.nz/assets/Uploads/daac08133a/defence-white-paper-2016.pdf>

Ministry of Defence, New Zealand. (2018). Strategic defence policy statement. Accessed 20 April 2020 from <http://www.nzdf.milnz/downloads/pdf/public-docs/2018/strategic-defence-policy-statement-2018p.df>

Moller, B. (1996). Common security and non-offensive defence as guidelines for defence planning and arms control? *International Journal of Peace Studies*, 1(2), 47--06.

Moller, B. (1998). Non-offensive defence in the Middle East. In B. Moller, G. Daniker, S. Lirnone, & I. A. Stivachtis (Eds.), *Non-offensive defence in the Middle East?* UNIDIR. New York and Geneva: United Nations.

Moller, B., & Wiberg, H. (1994). Introduction. In B. Moller, & H. Wiberg (Eds.), *Non-offensive defence for the twenty-first century*. San Francisco: Westview Press

Ng, H. (2019, July 5). No immediate threat to ships in straits of Malacca and Singapore, says MPA after China raises warning. *The Straits Times*. Accessed 20 April 2020 from <https://www.straitstimes.com/singapore/no-immediate-threats-to-ships-in-straits-of-malacca-and-singapore-says-mpa-after-china>

NZDF. (2019). New Zealand defence force annual report 2019. Accessed 20 April 2020 from <http://www.nzdfm.il.nz/downloads/pdf/public-docs/2019/nzdf-annual-report-2019-web.pdf>

Ong, V. C. (2011). Peripheral to Norm? The expeditionary role of the third generation Singapore Armed Forces. *Defence Studies*, 11(3), 541-558.

Stares, P., & Yacoubian, M. (2005, August 23). Terrorism as a virus. *The Washington Post*. Accessed 20 April 2020 from <https://www.washingtonpost.com/archive/opinions/2005/08/23/terrorism-as-virus/4d80814f-dedd-422f-865f-b375ef68c793/>

Stats NZ. (2020). Overseas merchandise trade: December 2019. Accessed 20 April 2020 from <https://www.stats.govt.nz/information-releases/overseas-merchandise-trade-december-2019>

Tamkin, E. (2019, March 20). New Zealand is one of the world's happiest countries. That also makes it resilient. *The Washington Post*. Accessed 20 April 2020 from <https://www.washingtonpost.com/world/2019/03/20/new-zealand-is-one-worlds-happiest-countries-that-also-makes-it-resilient/>

The second world war at home. (2020). In NZ history. Accessed 20 April 2020 from <https://nzhistory.govt.nz/war/second-world-war-at-home/challenges>

Waltz, K. N. (1979). *Theory of international politics*. New York: McGraw-Hill.

Wheeler, N.J., & Booth, K. (1992). *The security dilemma*. In J. Baylis & N. J. Rengger (Eds.), *Dilemmas in world politics*. Oxford: Clarendon Press.

White House. (2006, September). *National strategy for combating terrorism*. Washington, DC GPO.

## ENDNOTES

1. Fischer, D., & Bloomgarden, A. (1989). Non-offensive defense. *Peace Review*, 1(2), 7- 11. <https://doi.org/10.1080/10402658908425489>
2. Waltz, K. N. (1979). *Theory of international politics*. New York: McGraw-Hill.
3. Flanagan, S. (1988). Nonoffensive defense is overrated. *Bulletin of the Atomic Scientists: Nonoffensive Defense*, 44(7), 46-48. <https://doi.org/10.1080/00963402.1988.11456201>
4. Crawford, N.C., & Lutz, C. (2019, November 13). Human cost of post-9/11 wars. 20 years of war: A cost of war research series. Accessed 20 April 2020 from <https://wat.son.browne.du/costsofwarfiles/cow/imcelpapers/2019/Direct%20War%20Deaths%20COW%20Estimate%20November%2013%202109%20FINAL.pdf>
5. Wheeler, N.J., & Booth, K. (1992). *The security dilemma*. In J. Baylis & N. J. Rengger (Eds.), *Dilemmas in world politics*. Oxford: Clarendon Press.
6. Moller, B., & Wiberg, H. (1994). Introduction. In B. Moller, & H. Wiberg (Eds.), *Non-offensive defence for the twenty-first century*. San Francisco: Westview Press
7. Barnaby, F., & Boeker, E. (1988). Non-nuclear, non-provocative defence for Europe. In P.T. Hopmann & F. Barnaby (Eds.), *Rethinking the nuclear weapons dilemma in Europe*. New York: St. Martin's Press.
8. Moller, B. (1996). Common security and non-offensive defence as guidelines for defence planning and arms control? *International Journal of Peace Studies*, 1(2), 47-56.
9. Collins, J. M. (1998). *Military geography for professionals and the public*. Washington D.C: University of Nebraska Press
10. Huang, A. C. (2001). Transformation and refinement of Chinese military doctrine: Reflection and critique on the PLA's view. In J. Mulvenon & N. D. Yang (Eds.), *Seeking truth from facts: A retrospective on Chinese military studies in the post-Mao era*. Santa Monica, CA: RAND Corporation. <https://www.rand.org/content/dam/rand/pubs/conf/proceedings/CF160/CF160.ch6.pdf>
11. Butfoy, A. (1997). Offence-defence theory and the security dilemma: The problem with marginalizing the context. *Contemporary Security Policy*, 18(3), 38- 58. <https://doi.org/10.1080/13523269708404168>
12. Ibid.
13. Israel MFA. (n.d.) Israel's wars. Israel Ministry of Foreign Affairs. Accessed 20 April 2020 from <https://mfa.gov.il/MFA/AboutIsrael/History/Pages/Israel-Vars.aspx>
14. Moller, B. (1998). Non-offensive defence in the Middle East. In B. Moller, G. Daniker, S. Lirnone, & I. A. Stivachtis (Eds.), *Non-offensive defence in the Middle East? UNIDIR*. New York and Geneva: United Nations.
15. Collins, J. M. (1998). *Military geography for professionals and the public*. Washington D.C: University of Nebraska Press

16. Global Commission. (2019). A new world: The geopolitics of energy transformation. Accessed 20 April 2020 from [https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Jan/Global\\_commission\\_geopolitics\\_new\\_world\\_2019.pdf](https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Jan/Global_commission_geopolitics_new_world_2019.pdf)
17. Lawson, F. H. (2001). Rethinking the Iraqi Invasion of Kuwait. *Review of International Affairs*, 1(1), 1-20
18. Tamkin, E. (2019, March 20). New Zealand is one of the world's happiest countries. That also makes resilient. *The Washington Post*. Accessed 20 April 2020 from <https://www.washingtonpost.com/world/2019/03/20/new-zealand-is-one-worlds-happiest-countries-that-also-makes-it-resilient/>
19. The second world war at home. (2020). In NZ history. Accessed 20 April 2020 from <https://nzhistory.govt.nz/war/second-world-war-at-home/challenges>
20. NZDF. (2019). New Zealand defence force annual report 2019. Accessed 20 April 2020 from <http://www.nzdfm. il.nz/downloads/pdf/public-docs/2019/nzdf-annual-report-2019- web.pdf>
21. Stats NZ.(2020). Overseas merchandise trade: December 2019. Accessed 20 April 2020 from <https://www.stats.govt.nz/information-releases/overseas-merchandise-trade-december- 201>
22. NZDF. (2019). New Zealand defence force annual report 2019. Accessed 20 April 2020 from <http://www.nzdfm. il.nz/downloads/pdf/public-docs/2019/nzdf-annual-report-2019- web.pdf>
23. Chua, D. W. B. (2015, March 16). Konfrontasi: "Why it still matters to Singapore. RSIS Commentary 0 j4\_ <https://www.rsis.edu.2s/wp-content/uploads/2015/03/CO15054.pdf>
24. MICA. (2003). Water Talks - If only it could Singapore: Ministry of Information, Communications and the Arts Singapore
25. Desker, B. (2015, October 14). Challenging times in Singapore-Indonesia relations. RSIS Commentary 216. <https://www.rsis.edu.s2/wp-content/uploads/2015110/CO15216.pdf>
26. Jaipragas,B. (2018, December 5). Cross borders: Malaysia and Singapore continue to dispute air and sea boundaries. *South China :Morning Post*. Accessed 20 April 2020 from <https://www.scmp.com/news/asia/southeast-asia/article/2176552/cross-borders-malaysia-and-singapore-continue-dispute-air>
27. Ng, H. (2019, July 5). No immediate threat to ships in straits of Malacca and Singapore, says MPA after China raises warning. *The Straits Times*. Accessed 20 April 2020 from <https://www.straitstimes.com/singapore/no-immediate-threats-to-ships-in-straits-of- malacca-and-singapore-says-mpa-after-china>
28. Ong, \V. C. (2011). Peripheral to Norm? The expeditionary role of the third generation Singapore Armed Forces. *Defence Studies*, 11(3),541-558.
29. Ibid.
30. Crelinsten,R. (2014). Perspectives on counterterrorism: From stovepipes to a comprehensive approach. *Perspectives on Terrorism*,8(1), 2- 15.
31. White House. (2006, September). National strategy for combating terrorism. Washington, DC GPO.
32. Stares, P., & Yacoubian,M. (2005, August 23). Terrorism as a virus. *The Washington Post*. Accessed 20 April 2020 from <https://www.washingtonpost.com/archive/opinions/2005/08/23/terrorism-as- virus/4d80814f-dedd-422f-865f-b375ef68c793/>
33. Fukuyama, F.(2006, February 19). After neoconservatism. *The New York Times*. Accessed on 20 April 2020 from <https://www.nytimes.com/2006/0219/magazine/after- neoconservatism.html>



**LTC Phang Chun Chieh** is a Naval Officer by vocation. He has served in the submarine force since 2008 and is the Commanding Officer (Designate) of *RSS Impeccable*, one of the *Invincible*-class submarines. LTC Phang is currently training in Germany with his crew. He is also a SAF Postgraduate Award recipient and graduated with distinction from the United States Naval Postgraduate School with a Master of Science in Acoustic Engineering.

# THE 'CENTRE OF GRAVITY' CONCEPT IN CLAUSEWITZ'S 'ON WAR'

By MAJ Edward Khoo Chun Kiat

## ABSTRACT

In this essay, the author seeks to illustrate that even though the concept of centre of gravity may be abstract it can still be of use to military planners. He highlighted various problems with the concept such as how subjectivity and mistranslation which could lead to confusion and lack of utility. This is seen from the lack of a common definition of the centre of gravity, and how different conclusions can be derived from the multitude of conflicting methodologies that have arisen even in the same scenario. However, the author also explains how the centre of gravity can still be a useful concept as it helps planners understand increasingly complex operating environments by revealing relations within the multiple systems, distinguishing between the important and the peripheral. This therefore enables planners to focus actions on what are important and enhances efficiency.

*Keywords: CoG; War; Planning; Military; Strategy*

*"Everything in war is very simple, but the simplest thing is difficult."*

-Carl von Clausewitz

## WHAT IS CENTRE OF GRAVITY

'The hub of all power and movement, on which everything depends', is what we understood of the Centre of Gravity (CoG) concept, which was introduced by Carl von Clausewitz in his masterpiece, *'On War'* in 1832. Decades of researches, debates and operational applications have resulted in the numerous definitions of CoG available today. Even though CoG identification is considered the centerpiece of military planning, military practitioners still struggle with it, planners still misapply it, and commanders still search in vain for it. At best, this suggests that the concept is still an unsettled theory; at worst, it is not only irrelevant, it is a detrimental distraction.<sup>1</sup>

## ESSAY'S POSITION

In this essay, the author deliberates that the concept, although is abstract, is still of use to military planners. This is because, given the correct situation, with a clear definition and common methodology within the planning team, it still focuses on planning efforts.

The author first explains why the concept is abstract. He then elaborates on why critics are skeptical about the concept and argue that it is too abstract to be of use. Thereafter, he proceeds to demonstrate the

utility of the concept and its importance. Finally, the author goes on to discuss the limitations of the concept so that military practitioners and planners know when and how to apply it.

## ROOT PROBLEM & DIFFERING ACCEPTANCE OF CONCEPT

The original work by Clausewitz was written in German. Some have argued that Clausewitz's derivation of CoGs is intuitive in nature and as such, there lies a degree of subjectivity within.<sup>2</sup> Moreover, the widely used translation by Howard and Pret in 1984—"The hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed"—was criticised for its flaws in translation and is very much the culprit for much of the contentions in the contemporary understanding of the concept and its utility in the modern world.<sup>3</sup> The element of subjectivity and mistranslation has caused confusion, generated a diverse view on the concept, cast doubts on its application in the real world and divided opinions on its utility.

These opinions can be categorised into three groups of followers: the traditionalists, the rejectionists and the accommodators.<sup>4</sup> The Clausewitzian traditionalists are the advocates of Clausewitz's concepts, who believe that concepts raised by Clausewitz hold more weight than their actual utility. The rejectionists, however, are not troubled about the intellectuality of such concepts but are concerned with

its practicality. The accommodators, like the rejectionists, find utility of the concepts important to them as well. However, instead of outright rejecting the concepts, the accommodators try to resolve it by redefining the concept and applying it contextually.

## UNDERSTANDING THE ACHILLES OF THE COG CONCEPT

Critics reject the concept for three main reasons. Firstly, there are numerous definitions; it is fundamentally illogical for something so important to not have a common definition. Secondly, given the same scenario, the many methodologies may not derive the same CoG. Lastly, the difficulties in identifying correct CoGs across various planning level and aligning them to strategic CoG.

**Instead of focusing planning effort, the employment of service biased methods to derive CoG and all arriving at different conclusions, will only create disruption at the joint planning headquarters.**

### Multiple Definitions

Multiple definitions are one of the main stumbling blocks for the concept. Anything that is so controversial, debatable, unclear and continually changing is a weak foundation on which to build a plan.<sup>5</sup> Differences in their operating environments and services' capabilities resulted in respective services in the American military each having their own definition of the concept. For the Army and Navy typically though, in terms of a single CoG, which will reside at the core of land or sea power, and provides the source of physical and psychological capacity to fight.<sup>6</sup> The Air Force, on the other hand, envisioned multiple centres, each targeted from the air to paralyse an enemy. The Marine Corps has long regarded CoG as a critical vulnerability. Thus, the concept has assumed many guises over the years.<sup>7</sup>

Herein lies the drawback with the concept—the ambiguous representation of the concept resulted in different definitions by various services and thus, many

different CoGs identified in an operation. Instead of focusing the planning effort in defeating the enemy by targeting one CoG, the concept has generated multiple CoGs, created an incoherent planning headquarters, expended extra resources and time to defeat the adversary.

This was evident in *Operation Desert Storm*. In that operation, the absence of universal and well-developed CoG definitions resulted in poor unity of effort and synchronisation.<sup>8</sup> General Schwarzkopf, the overall campaign commander had derived three CoGs, two of which, the leadership and command and control assets coincides with General Horner, the commander of the Air Force for the operation. His last CoG was not considered by the Air Forces as a CoG and in addition, the Air Force had further identified 12 other targets as CoGs. Consequently, each service fought independently within their own domain, in a campaign riddled with frictions.<sup>9</sup> The very concept that was supposed to focus planning and operation effort, improve unity and efficiency, ironically divided the planning team's effort. One should not be surprised to see why critics are fast in condemning and rejecting the concept.

### Multiple Methodologies

We have witnessed multiple military professionals' efforts in refining the concept to operationalise it. Joseph Strange, a professor of Strategic Studies in the Marine Corps War College and a former Army officer and John Warden, a retired US (United States) Air Force (USAF) Colonel are two such examples. Each of them derived their own methodology. Warden's Strategic Ring Theory and Strange's Critical Capability – Critical Requirement – Critical Vulnerability Concept, from their own understanding and experience.

Each service approaches CoG analysis systematically, but nearly always ends in a tautology.<sup>10</sup> The problem is each of these efforts are biased due to the originator's experience with operation environments and an understanding of their past service's capabilities. In his Strategic Ring Theory, Warden established the five levels of system elements and that each level has a CoG.<sup>11</sup> Due to his experience and training with the Air Force, he advocates strategic bombing and is convinced that by hitting all the CoGs, it can neutralise the leadership and trigger paralysis. He connotes the possibility of hitting all the CoGs at once

because the Air Force can. On the other hand, Strange, being an Army officer, clearly understood that it is impossible for the Army to strike multiple CoGs at once. Thus, explains his logical and systematic means of identifying each of the critical factors and only to strike that one CoG, the one that mattered most at any given time. All the services claim to have procedures for identifying CoGs, but none of their doctrine states how to derive it.<sup>12</sup>

Smith, Jeter and Westgaard, in 2015, have used multiple approaches to study the CoG for Islamic State of Iraq and Syria (ISIS). They concluded that all methods provided structured processes for identifying CoGs and they arrived at a somewhat similar but not identical conclusion.<sup>13</sup> This compounds the problem. With different methods, planners at best can only arrive at a similar but not identical CoGs. Post World War I (WWI), most, if not all military operations involve joint participation. This is especially true in modern days. Instead of focusing planning effort, the employment of service biased methods to derive CoG and all arriving at different conclusions, will only create disruption at the joint planning headquarters. Yet again, it is little wonder why critics reject the concept.

**The tactical and operational  
CoGs are keys that open the doors  
to victory, but not victory itself.  
The strategic CoG is.**

## Multiple Levels Of Planning

'It is worth noting that Clausewitz does not distinguish among tactical, operational and strategic CoGs.'<sup>14</sup> However, due to the advancement in technology, the ways and means of warfare have changed considerably since Napoleon's time. Doctrinally, the planning of war is stratified across three levels—tactical, operational and strategic.<sup>15</sup> Today, CoG is seen to exist for every level of command.<sup>16</sup> This created two problems. Firstly, a few CoGs will be identified across the levels and it is the responsibility of the commander to strike the correct one.<sup>17</sup> Secondly, the CoGs across all levels must link, without which, the military will find itself involved in a conflict that is lacking purpose.<sup>18</sup>

The Vietnam War was an example at which the tactical and operational CoGs did not link with the strategic CoG. Primarily, the US military failed to understand that it was not a proxy war on ideology but rather a civil war, which resulted in the misidentification of a strategic CoG that was largely responsible for defeat.<sup>19</sup> The CoG is not Ho Chi Minh's government, but the peoples' will to not be ruled by a foreign power again. This is not a force that can be dissolved using military means, which is why tactical units' success do not translate to victory.

The tactical and operational CoGs are keys that open the doors to victory, but not victory itself. The strategic CoG is. Finding the correct CoG is challenging; to find a few stretching across the various planning levels and the need to align them with the strategic CoG is certainly an arduous task, which is why critics are skeptical on the concept.



President Kennedy's news conference of 23<sup>rd</sup> March, 1961.

## UTILITY OF THE COG CONCEPT

Despite the criticisms, the author believes that CoG remains applicable and will continue to do so because it still has utility. This utility is defined as the ability to contribute to planning by improving understanding, focusing planning and improving efficiency.<sup>20</sup> The roles of military planners are to identify goals, determine missions, assess comparative advantage and risk, calculate costs and benefits.<sup>21</sup> The correct identification of CoG precisely facilitates this. It helps planners to identify what needs to be done to achieve aims and consequently, to assess whether benefits are important enough to justify the associated costs and risks. It forms the foundation and provides the focus for planning.<sup>22</sup> Clearly, by identifying the correct CoG, it enhances understanding, focuses planning and improves efficiency.<sup>23</sup>

The identification of the correct CoG is paramount to the success of achieving the aim too. A good example would be General MacArthur's plan for the Battle of Inchon—hitting North Korea's weaker rear elements in order to break out from the Busan Perimeter and push the North Koreans back to the borders. The converse is true as well. The Japanese misidentified America's carrier groups in the Pacific as the CoG instead of her people's will and industrial

might. Had Japan not misjudged this and avoided the attack on Pearl Harbour, which triggered America's retaliation by participating in the war in the Pacific, the outcome of World War II (WWII) for the Japanese would have been very different.<sup>24</sup>

Since the end of the Vietnam War, we have witnessed the revival of the CoG concept, the many debates over its true meaning and its application in multiple operations by the world's leading military power, the US. All these efforts are proof that this age-old concept is still valuable for the military today. Denouncing the concept by claiming that it is abstract, oversimplifying things and it cannot be applied in today's complex environment do no justice to the concept. Changes in time, technology and modern military doctrines do not necessarily make the concept irrelevant, because the concept focuses on the art of planning, the bread and butter of military planners.<sup>25</sup>

The value of the concept will not be doubted once military professionals are able to utilise it productively. Therefore, the objective is to operationalise the concept successfully. However, over the years, literal interpretation of the concept led practitioners to misunderstand the deeper underlying ideas.<sup>26</sup> The challenge then is how to reverse this misconstrued understanding and confusion. The shift of



*Photograph of Battleship Row taken from a Japanese plane at the beginning of the attack (on Pearl Harbour). The explosion in the center is a torpedo strike on USS West Virginia. Two attacking Japanese planes can be seen: one over USS Neosho and one over the Naval Yard.*

definition from metaphors to language based on clarity, logic and precision, and testability by some Neo-Clausewitzian is one good effort to swing the motion in the right direction.<sup>27</sup>

**In such asymmetric warfare, the ideas of success and failures are intangible, the CoG lies in the hearts and minds of the population, something that cannot be defeated by military might.**

## LIMITATIONS OF THE CONCEPT

Unlike the laws of physics, a concept remains a concept and has its limitation. It cannot be applied universally and timelessly. It is only right for practitioners to understand these limitations before adopting it, failure of which will only distract the planning team by leading them on a wild goose chase.

Firstly, the CoG concept cannot be applied for every type of war. It is applicable to wars designed to defeat adversaries. In such wars, military and political objectives are essentially complementary. Whereas in limited wars, CoG tend to compete with restrictive political objectives.<sup>28</sup> The First Gulf War was a conflict with limited aims and the concept should not have been applied. General Schwarzkopf's notion of the enemy's CoG did not accord with those of General Horner. As a result, the planners were more concerned about what the CoGs were, as opposed to what to do with it. The force fitting concept was unnecessary as translating the war's strategic objectives, the expulsion of Iraqi forces from Kuwait, into operational and tactical objectives would still have identified the capabilities the coalition forces had to defeat in order to be successful.<sup>29</sup> Unless political aim and military aim are in line with the goal of rendering the enemy defenceless, searching for CoG is unnecessary and possibly counterproductive. In a limited war, the collapse of an opponent might not serve the political purposes and could run counter to them.<sup>30</sup>

Secondly, as it is impossible to know before hand with any degree of certainty whether the CoG has been correctly determined due to the uncertainty nature of war, planners must be cognisant that CoG can change and should not be too adamant on fixing to only those that have been identified.<sup>31</sup> The lack of focus caused by inter-service definition problems is not the worst outcome of the use of CoG. Instead, the telescopic focus to a single CoG but getting it wrong and declining to adjust is.<sup>32</sup> Leaders and planners must remember that they are handling a dynamic situation and not observing a static system. They are fighting a thinking enemy and not one sitting duck. In 2005, General Casey's team misidentified the Iraqi government as the true CoG. The insurgency in Iraq rose to a new level of violence in 2006.<sup>33</sup> The situation only improved after Petraeus took command and changed the COG to focus on a population centric counterinsurgency strategy. The fixated minds of the first team caused them to disregard new developments, especially when it is something that did not fit their initial assessment. This resulted in dire consequences and will continue to do so, if planners do not understand that COG can change.



*Public memorials for the victims died in the November 2015 Paris attacks, and police near the scenes of some of the attacks. November 2015 Paris attacks is part of Terrorism in Europe and the spillover of the Syrian Civil War.*

Finally, transnational terrorism threat is different in nature as compared to a conventional security threat. The battling of ideology is not a threat that can be answered with military strength alone. In addition, technology and social media have allowed the enemy to be connected, yet independent from each other. Under such circumstances, there is limited utility for the CoG concept. Firstly, the lack of overarching system means there is no focal point at which military force can target. Destroying ISIS cells in Europe does no harm to the cells in Southeast Asia. Secondly, the effectiveness of using military force to fight an ideology comes into question. In fact, it is counterproductive—the more tactical and operational success you gain, the further you are away from strategic victory. In such asymmetric warfare, the ideas of success and failures are intangible, the CoG lies in the hearts and minds of the population, something that cannot be defeated by military might.

## CONCLUSION

The CoG concept remains abstract but is still and will continue to be relevant because it has utility to planners. It helps them to understand increasingly complex operating environments by revealing relations within the multiple systems, distinguishing between the important and the peripheral. This enables planners to focus actions on what are important and enhances efficiency. However, this is, after all, a concept. In the fast paced volatility, uncertainty, complexity and ambiguity (VUCA) environment, dealing with dynamic enemies, military practitioners must understand its limitations. Today's military would do well to ensure that those trained in identifying CoG are taught to know how and when to use it, rather than meaninglessly forced fitting it into every situation, which may result in frustration and only then, to lament the concept is too abstract to be of use.

## BIBLIOGRAPHY

- Belanger, J. A. (1999). *Causes Of The Vietnam War: An Academic Look At Wilsonism And Cold War Effects*. Alabama: Air Command And Staff College.
- Dixon, R. (2015). Clausewitz, Center of Gravity, and the Confusion of a Generation of Planners. *Small Wars Journal*.
- Echevarria II, A. J. (2003). Clausewitz'S Centre Of Gravity It's Not What We Thought. *Naval War College Review*.
- Echevarria II, A. J. (2003). Reigning in the Centre of Gravity Concept. *Air and Space Power*, 87.
- Echevarria II, A. J. (2004). Centre of Gravity Recommendations for Joint Doctrine. *Joint Force Quarterly*.
- Echevarria II, A. J. (2012). Clausewit'z Centre of Gravity Legacy. *Infinity Journal*, pp. 4-7.
- Eikmeier, D. C. (2016). Let's Fix or Kill the Centre of Gravity Concept. *Joint Force Quarterly*.
- Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
- Giles, P. K., & Galvin, T. P. (1996). *Centre of Gravity Determination Analysis and Application*. Pennsylvania: Centre for Strategic Leadership U.S. Army War College.
- Howard, M., & Paret, P. (1989). *Carl von Clausewitz, On War*. Princeton: Princeton University Press.
- Keaney, T. A., & Cohen, E. A. (1993). *Gulf War Air Power Survey Summary Report*. Washington D.C.: US Government Printing Office.
- Leonard, S. (2019, March 5). *That Clausewitz-Is-Irrelevant "Hot Take " Isn 'T Blasphemous. It 'S Just Wrong*. Retrieved from Modern War Institute At West Point: <https://mwi.usma.edu/clausewitz-irrelevant-hot-take-isnt-blasphemous-just-wrong/>
- Leonhard, R. (1991). *The Art of Maneuver Maneuver-Warfare Theory and Airland Battle*. New York: Ballantine Books.
- Mahnken, T. K. (2000). Strategic Theory. In J. Baylis, J. J. Wirtz, & C. S. Gray, *Strategy in the Contemporary World* (pp. 52-64). New York: Oxford University Press.
- Peterson, G. C. (1994). *Centre of Gravity: A Most Important Concept Mostly Misunderstood*. Newport: Naval War College.
- Smith, D. J., Jeter, K., & Westgaard, O. (2015). Three Approaches to Centre of Gravity Analysis The Islamic State of Iraq and the Levant. *Joint Force Quarterly*.
- Strange, J. L. (1996). *Perspectives on Warfighting: Centers of Gravity & Critical Vulnerabilities*. Quantico: Marine Corps University.
- Strange, J. L., & Iron, R. (2004). Center of Gravity What Clausewitz Really Meant. *Joint Force Quarterly*.
- Warden III, J. A. (1995). The Enemy As a System. *Airpower Journal*, 40-55.

## ENDNOTES

1. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*
2. Echevarria II, A. J. (2012). Clausewit'z Centre of Gravity Legacy. *Infinity Journal*, pp. 4-7.
3. Eikmeier, D. C. (2016). Let's Fix or Kill the Centre of Gravity Concept. *Joint Force Quarterly*.
4. Ibid.
5. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
6. Echevarria II, A. J. (2003). Reigning in the Centre of Gravity Concept. *Air and Space Power*, 87.
7. Echevarria II, A. J. (2004). Centre of Gravity Recommendations for Joint Doctrine. *Joint Force Quarterly*.
8. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
9. Ibid.
10. Dixon, R. (2015). Clausewitz, Center of Gravity, and the Confusion of a Generation of Planners. *Small Wars Journal*.
11. Warden III, J. A. (1995). The Enemy As a System. *Airpower Journal*, 40-55.

12. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
13. Smith, D. J., Jeter, K., & Westgaard, O. (2015). Three Approaches to Centre of Gravity Analysis The Islamic State of Iraq and the Levant. *Joint Force Quarterly*.
14. Echevarria II, A. J. (2003). Clausewitz'S Centre Of Gravity It's Not What We Thought. *Naval War College Review*.
15. Leonhard, R. (1991). *The Art of Maneuver Maneuver-Warfare Theory and Airland Battle*. New York: Ballantine Books.
16. Strange, J. L. (1996). *Perspectives on Warfighting: Centers of Gravity & Critical Vulnerabilities*. Quantico: Marine Corps University.
17. Warden III, J. A. (1995). The Enemy As a System. *Airpower Journal*, 40-55.
18. Giles, P. K., & Galvin, T. P. (1996). *Centre of Gravity Determination Analysis and Application*. Pennsylvania: Centre for Strategic Leadership U.S. Army War College.
19. Belanger, J. A. (1999). *Causes Of The Vietnam War: An Academic Look At Wilsoniasm And Cold War Effects*. Alabama: Air Command And Staff College.
- Peterson, G. C. (1994). *Centre of Gravity: A Most Important Concept Mostly Misunderstood*. Newport: Naval War College.
20. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
21. Mahnken, T. K. (2000). Strategic Theory. In J. Baylis, J. J. Wirtz, & C. S. Gray, *Strategy in the Contemporary World* (pp. 52-64). New York: Oxford University Press.
22. Giles, P. K., & Galvin, T. P. (1996). *Centre of Gravity Determination Analysis and Application*. Pennsylvania: Centre for Strategic Leadership U.S. Army War College.
23. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
24. Giles, P. K., & Galvin, T. P. (1996). *Centre of Gravity Determination Analysis and Application*. Pennsylvania: Centre for Strategic Leadership U.S. Army War College.
25. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
26. Leonard, S. (2019, March 5). *That Clausewitz-Is-Irrelevant "Hot Take " Isn 'T Blasphemous. It 'S Just Wrong*. Retrieved from Modern War Institute At West Point: <https://mwi.usma.edu/clausewitz-irrelevant-hot-take-isnt-blasphemous-just-wrong/>
27. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.
28. Echevarria II, A. J. (2003). Reigning in the Centre of Gravity Concept. *Air and Space Power*, 87.
29. Ibid.
30. Echevarria II, A. J. (2012). Clausewit'z Centre of Gravity Legacy. *Infinity Journal*, pp. 4-7.
31. Ibid.
32. Dixon, R. (2015). Clausewitz, Center of Gravity, and the Confusion of a Generation of Planners. *Small Wars Journal*.
33. Eikmeier, D. C. (2017). The Center of Gravity Still Relevant After All These Years. *Military Review*.



**MAJ Edward Khoo Chun Kiat** is an Infantry Officer by vocation and is currently the Intelligence Officer of 2<sup>nd</sup> Singapore Infantry Brigade. He graduated from the National University of Singapore with a Bachelor of Science (Honours) in Life Sciences with Specialisation in Environmental Biology.

# CAN A SMALL STATE CHALLENGE A MUCH LARGER STATE OR A COLLECTION OF ENEMY STATES?

By ME5 Lim Sher Hern

## ABSTRACT

This essay examines how, despite the odds stacked against them, small states can still employ an effective conventional deterrence strategy. The author first explores the concept of deterrence before discussing the issue of deterrence through military superiority. He then analyses other approaches to deterrence, such as total defence and alliance. The author also highlights that it is in the interests of small states to pursue some form of deterrence against potential adversaries because an armed conflict can threaten their very existence. However, the author concludes that deterrence is not a permanent solution to security problems. It is a dynamic posture that has to be maintained to ensure that the state does not pay a heavy price for the devastation of war. In his opinion, successful deterrence is simply an extension of time to address the underlying geopolitical issues.

*Keywords: Deterrence; Nuclear; Dissuade; Strategies; DIME*

## INTRODUCTION

Small states are arbitrarily defined using criteria such as land area, population, Gross Domestic Product (GDP) or even the extent of their influence. It is not easy to find a consensus on the most fitting definition, if one even exists. Danish political analyst Erling Bjol points out that the concept of a small state does not mean anything when considered in isolation of an international system.<sup>1</sup> He says that 'a state is only small in relation to a greater one.'<sup>2</sup> Hence, my consideration of small states in this essay would be those that exhibit stark asymmetry when compared with their adversaries.

Regardless, most would agree that small states have the odds stacked against them. The late Singaporean statesman Lee Kuan Yew believed that small states will always be particularly vulnerable to global happenings.<sup>3</sup> They perform few significant roles in the international system, and the world will carry on even without their existence.<sup>4</sup> History has illustrated the decline of many small states including Athens, Sparta and Venice, and their consequent absorption by their larger neighbours.<sup>5</sup>

Given a small state's inherent vulnerabilities, there is good reason to doubt its ability to deter a much larger adversary or a collection of enemy states. American political scientist John Mearsheimer recognises that the degree of asymmetry may be 'so

great that the attacker does not have the slightest doubt that he will succeed on the battlefield.'<sup>6</sup> In this instance, 'deterrence does not really apply.'<sup>7</sup> Nonetheless, I posit that being small is not necessarily a foregone conclusion. It is still possible for a small state to operationalise an effective conventional deterrence strategy.

The focus of this essay shall be on conventional deterrence because most small states do not have nuclear weapons, and therefore cannot employ nuclear deterrence strategies. There is also a fundamental assumption that adversarial states are rational actors who make decisions based on utility, and hence can be deterred. The assumption of rationality is the cornerstone of deterrence theory.

The essay first discusses the concept of deterrence and the conditions for successful deterrence. Next, it examines the examples of Israel, Switzerland and Norway in their demonstrations of effective deterrence through military superiority, a whole-of-society defence strategy, and an alliance's support. Finally, the essay explores the challenges of deterrence for small states, including the limitations of conventional deterrence. Despite these challenges, it is still possible and in the interests of small states to pursue the deterrence of larger adversaries because, for most, war is not an option.

## CONCEPT OF DETERRENCE

Deterrence can be defined as the power to dissuade an adversary from performing an action by showing that the cost and risk of his action outweigh his prospective gain.<sup>8</sup> Essentially, classical deterrence theory focuses on a threat-based approach through the creation of military capability sufficient to convince an adversary not to undertake an act of aggression.<sup>9</sup> Deterrence succeeds when an adversary believes that his military action will fail or result in dire consequences, hence refraining from that action.

There are two fundamental but non-mutually exclusive approaches to deterrence. *Deterrence by denial* strategies seek to convince an adversary that any act of aggression is unlikely to succeed. Political scientist Michael Mazarr views *deterrence by denial* as representative of a state's capability, intention and effort to defend a commitment.<sup>10</sup> Any attack on the commitment, if not defeated, would be protracted and costly.<sup>11</sup>

On the other hand, *deterrence by punishment* strategies threaten severe punishment for an act of aggression.<sup>12</sup> Notably, the 'focus of deterrence by punishment is not the direct defence of the contested commitment but rather threats of wider punishment' that would make the attack disproportionately costly and irrational to the adversary.<sup>13</sup> *Deterrence by punishment* is typically associated with the possession of nuclear weapons as a deterrent, because the employment of nuclear weapons promise complete destruction of the adversary.<sup>14</sup> There are no reliable means to defend against nuclear weapons or mitigate their effects.<sup>15</sup> Thus, a nuclear state can threaten punishment of unacceptable cost if an attack occurs. For the longest time, conventional weapons were unable to achieve similar effects as nuclear weapons. Hence, for the most part, non- nuclear small states could not reliably inflict punishment and had to rely on conventional *deterrence by denial* strategies. The advent of highly destructive precision-guided conventional munitions has changed this equation.

A successful deterrence strategy has to satisfy criteria in the aspects of (1) capability, (2) credibility and; (3) communication. First, the state must have the military capability to repel and retaliate against the adversary to deny its objectives.<sup>16</sup> Second, the state

must convince the adversary that it has credibility because it has the political will to act if threatened.<sup>17</sup> Third, the state must clearly communicate the cost to the adversary, including its capability, will, and responses should certain boundaries (also known as 'red lines') be crossed.<sup>18</sup> Crucially, these boundaries and threatened responses must appear credible to the adversary and be worth going to war for, should deterrence fail.<sup>19</sup>

## ACHIEVING DETERRENCE THROUGH MILITARY SUPERIORITY

Israel is an example of a small state that has kept a collection of larger Arab states at bay through its military superiority, which presents a massive cost to potential adversaries for any attack on it. This is an achievement considering Israel's geographic asymmetry relative to the neighbours that had threatened it with complete eradication. Israel is dwarfed and surrounded by Egypt, Lebanon, Syria and Jordan. It has little strategic depth. The Israel Defence Forces (IDF) would be outnumbered by an aggregated Arab coalition. Israeli strategic thought recognises these constraints and assumes that 'Israel would always engage its enemies from an inferior position in terms of territory, resources, and tolerance to casualties and to international pressure.'<sup>20</sup>

Every episodic success in preventing the adversary from achieving its goals and eroding its military capabilities alters its cost-benefit calculus and achieves deterrence for the next round.

Nevertheless, Israel has created 'reverse asymmetry' by capitalising on its technological superiority to compensate for its numerical disadvantage.<sup>21</sup> It has been at the forefront of military innovation, which has preserved its strategic edge for the offence with smart weapons such as unmanned combat systems and vehicles, integrated electronic warfare systems and precision-guided munitions.<sup>22</sup> Israel also leads in the research and development of integrated early warning and air defence systems, and

has built layered anti-missile defence systems such as the *Iron Dome* which can deal with a range of aerial threats from tactical rockets to intercontinental ballistic missiles.<sup>23</sup>

Israel's offensive and defensive capabilities contribute to both its *deterrence by denial* and by *punishment*. Israel's ability to strike its adversaries preemptively and defend against incoming threats achieve *deterrence by denial* by denying its adversaries success on the battlefield. At the same time, Israel has threatened *punishment* through massive retaliation targeted at adversary cities.<sup>24</sup> *Deterrence by punishment* is typically associated with nuclear weapons, but Israel's conventional precision strike capabilities can ensure the destruction of its adversaries' strategic targets.<sup>25</sup> Its adversaries have little means to stop these strategic strikes. However, it should be noted that Israel's deliberate ambiguity over its possession of nuclear weapons bolsters its ability to *deter by punishment* as well.<sup>26</sup>

Pertinently, what stands out in the Israeli case is that every Israeli victory on the battlefield is seen to be a communication of its credibility and capability. By most Western definitions, the very use of force implies that deterrence has failed, and the assumptions it was based on were incorrect.<sup>27</sup> The Israeli approach, on the

other hand, believes that deterrence cannot achieve zero violence. Deterrence is not permanent and has to be maintained through 'episodic uses of force.'<sup>28</sup> Every episodic success in preventing the adversary from achieving its goals and eroding its military capabilities alters its cost-benefit calculus and achieves deterrence for the next round.<sup>29</sup> This means that violence is not completely eradicated but is postponed with reduced magnitude.<sup>30</sup> Dmitry Adamsky aptly describes Israeli deterrence as 'The sword by itself does not establish credibility: it should be constantly bloodied to maintain deterrence.'<sup>31</sup>

## ACHIEVING DETERRENCE THROUGH TOTAL DEFENCE

Aside from pursuing military superiority, small states can adopt a *Total Defence* strategy to deter larger adversaries. A *Total Defence* strategy is a whole-of-society concept that co-ordinates defence planning across multiple domains, including political, military, economic and social, to achieve deterrence.<sup>32</sup> Fundamentally, this concept enlists efforts from all sectors of society to work around the constraints of a small state, such as its lack of military parity and strategic depth, to maximise the prospective cost of an attack in order to dissuade a potential adversary.



Completed, Israel's nuclear facility, the Dimona complex as seen by US Corona satellite on 11<sup>th</sup> November, 1968.

Switzerland, a small state of about 8.5 million people, is one of a few neutral European states that have adopted a variant of *Total Defence* as its security strategy. Termed by the Swiss as *General Defence*, this strategy seeks to safeguard peace and neutrality, prevent armed attacks against Switzerland, and preserve its independence and sovereignty.<sup>33</sup> The preservation of peace by acquiescing territory or complying with foreign pressure is not acceptable.

The objective of *General Defence* is the *dissuasion* of aggression. The term *deterrence* is avoided because the Swiss associate it with an offensive threat of retaliation against an adversary following an attack, which is deemed to be beyond their military means and incompatible with their neutrality.<sup>34</sup> Instead, the Swiss perceive *dissuasion* as the 'ability to avoid war through a combination of militarily credible preparedness, public confidence in and support of an active military defence, and protection of the civil population.'<sup>35</sup> In practice, *dissuasion* includes: (1) maximising the costs of an attack; and (2) minimising the gains of an aggressor from an attack.<sup>36</sup> This, in the author's opinion, is essentially *deterrence by denial* disguised with inoffensive overtures.

To maximise the costs of an attack, Switzerland signals that its military, supported by whole-of-society, is credible and capable of resisting any attack. The largely conscripted Swiss Army can mobilise 650,000 soldiers in 48 hours, and, considering the state's small land mass, this achieves the highest density of boots on the ground in Europe.<sup>37</sup> Extensive military fortifications amid mountainous terrain also favour the defenders.

On the economic front, despite Switzerland's landlocked geography and dependence on external sources for food and raw materials, its diversified supply chains and a national stockpile of essentials can sustain it through prolonged isolation.<sup>38</sup> As for the civil dimension, the Swiss civil defence system has sufficient shelter space to protect 90% of its population from anything short of a full-scale nuclear war.<sup>39</sup> Crucially, this allows Switzerland to resist external intimidation and blackmail because it is confident of protecting its soldiers and their families.<sup>40</sup>

Moreover, in a bid to minimise prospective gains to the adversary, Switzerland is prepared to destroy

industrial plants, goods, infrastructure and transportation systems to deny enemy usage.<sup>41</sup> In the event that the Swiss military is overwhelmed, the government has pledged to continue underground resistance. In this context, where every Swiss male has received military training and keeps his personal weapon at home, the threat of guerilla warfare is credible.<sup>42</sup> The only gain to the adversary would be its occupation of a hostile territory devoid of utility, with continued armed resistance waged by a determined population.<sup>43</sup>

Finally, Switzerland's history strengthens the case for small states to adopt a *Total Defence* strategy to deter larger adversaries. It was the only Central European state that Germany did not invade during the Second World War for reasons unknown. Nonetheless, a reasonable conjecture would be that Switzerland had few benefits to offer for the potentially costly effort to invade it. Hence, in the larger scheme of German war efforts, an invasion of Switzerland was not a priority.

## ACHIEVING DETERRENCE THROUGH ALLIANCE

Small states can also deter larger adversaries through military alliances. These bilateral (e.g. with a major power) or multilateral (e.g. with a collection of regional states) alliances are based on shared security interests. Deterrence is achieved when the aggressor recognises that an attack on the small state will elicit a military response from the alliance, and decides that the prospective gains from this course of action do not justify its cost.

Norway is an example in its longstanding dependence on the North Atlantic Treaty Organisation (NATO) for capable and credible deterrence against Russia.<sup>44</sup> Its geographical location beside an outsized Russia, lack of strategic depth and relative military inferiority drive its dual-track approach of deterrence and *détente* towards Russia. The former is one of extended deterrence that promises both *denial* and *punishment*. Firstly, Norway will receive support from Allied forces to stop the adversary from achieving its objectives in a conflict. Secondly, it draws on the nuclear deterrence provided by the US and other nuclear-armed allies.

**Deterrence is achieved when the aggressor recognises that an attack on the small state will elicit a military response from the alliance, and decides that the prospective gains from this course of action do not justify its cost.**

Norway's dependence on the larger NATO ambit does not mean that its own military capability is neglected. Alliance partnership works both ways. Norway's ability to deter aggression and defend against limited attacks without Allied support strengthens NATO's collective deterrence.<sup>45</sup> Similarly, the ability of NATO members to deploy and operate in Norway enhances the country's deterrence. There is consensus that the Norwegian Armed Forces 'punches above its weight' qualitatively with its professional training and access to high-end technology, despite lacking the quantitative figures afforded by its larger allies like the US or UK.<sup>46</sup> More importantly, Norway's access to cutting-edge systems like the F-35A Joint Strike Fighter

and P-8 Poseidon maritime patrol aircraft offers strategic and operational benefits in their interoperability with and connectivity to other NATO systems.<sup>47</sup> Coupled with Norway's large-scale military exercises with its NATO allies and Nordic neighbours to hone tactical integration and NATO's ability to deploy to the Arctic, they signal the alliance's commitment to defend Norway and its capability to operate effectively as an integrated fighting force.<sup>48</sup>

Significantly, Norway can rely on NATO for its defence because NATO member states collectively recognise the strategic importance of securing Norwegian territory, airspace and waters. There is a convergence in their strategic interests. For Norway, a Russian invasion is unlikely, but increasing Russian assertiveness over the Arctic region and its natural resources directly threatens Norwegian economic security.<sup>49</sup> As for NATO's European members like Denmark, Iceland and the United Kingdom (UK), Norway sits between them and Russia. The deterrence of Russian aggression against Norway directly contributes to their security. Moreover, members like Germany, the UK and the Netherlands import energy from Norway, and their companies are vested in the Norwegian energy sector.<sup>50</sup>



A British Army Scimitar reconnaissance vehicle during Exercise COLD WINTER '87 in Norway.

Besides, NATO members recognise the military significance of the Arctic region as a critical channel between Russia and the North Atlantic Ocean.<sup>51</sup> This channel facilitates Russia's deployment of its ballistic missile submarines, an essential component of its nuclear deterrence capability, and potentially its disruption of the movement of NATO forces and sea lines of communication across the North Atlantic Ocean. Thus, the collective deterrence of Russia in the Arctic contributes to the continued security of Allied operations and interests in the region.

## CHALLENGES WITH DETERRENCE FOR SMALL STATES

Nevertheless, small states face an uphill struggle in deterring larger adversaries due to their inherent vulnerabilities. Kuwait is perhaps a classic example of a small state that has little ability to deter its larger neighbours, and has to seek protection from a larger security partner. Unfortunately, there are risks to relying on someone else for defence, particularly in the absence of a mutual defence treaty and if the security partner's commitment to protecting shared interests is not clear. Kuwait paid dearly in 1990 when Iraqi troops invaded, swept away its limited resistance, and conquered the state within hours.<sup>52</sup> Deterrence had

failed because Washington's communications with Iraq preceding the invasion were "ambiguous and contradictory."<sup>53</sup> Saddam Hussein did not perceive the United States' (US) commitment to defend Kuwait to be credible.

There are also inherent deficiencies in conventional deterrence strategies. For instance, there are challenges for a small state to establish *deterrence by denial* or *punishment* because of the nature of conventional capabilities. The state's ability to impose a cost on its adversary is dependent on the weapons it possesses, its technical competencies in their application, and the presence of enemy counter-measures.<sup>54</sup> A potential adversary may view conventional deterrents as 'contestable costs' because there is a prospect of a technical, tactical or operational solution that would degrade their effectiveness.<sup>55</sup> This was the case in Egypt's circumvention of Israel's conventional deterrents, primarily the IDF's air superiority and armour capabilities, in 1973. Egypt's operational strategy to neutralise Israeli armour with a wall of anti-tank guided missiles and Israeli air power with a tactical shield of surface-to-air missiles degraded Israel's ability to inflict prohibitive costs, thereby making Egypt's initiation of the Yom Kippur War possible.<sup>56</sup>



Kuwaiti oil fires set by retreating Iraqi forces in 1991.

**The state's ability to impose a cost on its adversary is dependent on the weapons it possesses, its technical competencies in their application, and the presence of enemy counter-measures.**

Moreover, deterrence theory is premised on rationality, but value perception is subjective. In the lead up to the Yom Kippur War, Israel recognised its overwhelming military superiority and was convinced that war would not be a viable option for its Arab adversaries unless victory was certain.<sup>57</sup> However, the Arab states had a different logic. They reasoned that they could make political gains even if they lost battles. They would survive even if they lost a war. Israel failed to realise that the larger risk appetite of the Arab states changed their cost-benefit calculus until it was too late. Hence, it is often easy to assume that deterrence is working when it is not challenged.<sup>58</sup>

This highlights a general limitation with the study of deterrence. It is easier to identify deterrence failures when the use of force occurs, such as in Kuwait. On the other hand, it is way more difficult to find empirical support for conventional deterrence successes, much less to prescribe a definitive strategy for success for

small states. Many factors influence the avoidance of conflict.<sup>59</sup> It is extremely difficult to isolate deterrence as the key success factor.

Finally, in today's volatile security landscape, it is difficult to envision how a small state can reliably deter a larger adversary from threatening it through hybrid and non-conventional means that fall below the threshold of war.

## CONCLUSION

Despite the deficiencies in deterrence theory, it is definitely in the interest of small states to pursue some form of deterrence against potential adversaries because an armed conflict can threaten their very existence. As discussed, the pursuit of military superiority, whole-of-society defence, and an alliance with a major power are viable means for a small state to impose a hefty cost on armed aggression, which may consequently dissuade an adversary from this course of action. The adoption of one or more of these means depends on the state's context. For instance, an alliance might be effective (unlike Kuwait's case) if there is intimate alignment of strategic interests and culture. That said, deterrence is not a permanent solution to security problems. It is a dynamic posture that has to be maintained to ensure that the cost of war is not contestable. Successful deterrence is simply an extension of time to address the underlying geopolitical issues.<sup>60</sup>

## BIBLIOGRAPHY

- Adamsky, Dmitry (Dima). 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force'. *Security Studies* 26, no. 1 (2017): 157–84.
- Ang Cheng Guan. 'Singapore's Conception of Security'. In *Perspectives on the Security of Singapore: The First 50 Years*, 3–20. Singapore: World Scientific, 2016.
- Bar, Shmuel. 'Israeli Strategic Deterrence Doctrine and Practice'. *Comparative Strategy* 39, no. 4 (2020): 321–53.
- Black, James, Stephen Flanagan, Gene Germanovich, Ruth Harris, David Ochmanek, Marina Favaro, Katerina Galai, and Emily Ryen Gloinson. 'Enhancing Deterrence and Defence on NATO's Northern Flank'. Santa Monica, Calif: RAND Corporation, 2020.
- Bowers, Ian. 'IFS Insights 9/2018: Small State Deterrence in the Contemporary World'.
- Norwegian Institute for Defence Studies, 2018.
- Chorev, Moni. 'Surprise Attack. The Case of the Yom-Kippur War'. Washington, DC: National Defence University, 1996.
- Fischer, Dietrich. 'Invulnerability without Threat: The Swiss Concept of General Defense'. *Journal of Peace Research* 19, no. 3 (1982): 205–25.
- Folland, Rolf. 'Arctic Security: Deterrence and Détente in the High North'. The Arctic Institute, 30 March 2021. <https://www.thearcticinstitute.org/arctic-security- deterrence-detente-high-north/>.
- Golov, Avner. 'Israeli Deterrence in the 21st Century'. Tel Aviv: Institute for National Security Studies, June 2016.
- Gotkowska, Justyna. 'Norway and the Bear: Norwegian Defence Policy - Lessons for the Baltic Sea Region'. Point of View. Warsaw, Poland: Ośrodek Studiów Wschodnich, January 2014.
- Haffa Jr, Robert P. 'The Future of Conventional Deterrence: Strategies for Great Power Competition'. *Strategic Studies Quarterly*, Winter 2018.
- Harknett, Richard J. 'The Logic of Conventional Deterrence and the End of the Cold War'. *Security Studies* 4, no. 1 (1994): 86–114.
- Inbar, Efraim, and Shmuel Sandler. 'Israel's Deterrence Strategy Revisited'. *Security Studies* 3, no. 2 (1993): 330–58.
- Kam Kai Qing. 'The Viability of Deterrence Strategies for Non-Nuclear States'. *POINTER, Journal of the Singapore Armed Forces* 44, no. 1 (2018): 11–20.
- Lee, Li Huat. 'Will Strengthening the SAF Mean Strengthening Singapore's Deterrence as a Non-Nuclear State?' *POINTER, Journal of the Singapore Armed Forces* 41, no. 4 (2015): 21–32.
- Lee Yimou, David Lague, and Ben Blanchard. 'China Launches "Gray-Zone" Warfare to Subdue Taiwan'. *Reuters*, 10 December 2020. <https://www.reuters.com/investigates/special-report/hongkong-taiwan- military/>.
- Mazarr, Michael J. 'Understanding Deterrence'. Perspective. RAND Corporation, 2018.
- Nilsen, Thomas. 'Norway to Host Biggest Exercise inside Arctic Circle since Cold War'. *The Barents Observer*, 14 April 2021. <https://thebarentsobserver.com/en/security/2021/04/norway-host-biggest-exercise-inside-arctic-circle-cold-war>.
- Raska, Michael. 'Creating Reverse Asymmetry: Patterns of IDF's Military Innovation'. RSIS Commentaries. S.Rajaratnam School of International Studies, 5 December 2012.
- Snyder, Glenn Herald. *Deterrence and Defense: Toward a Theory of National Security*. Princeton, New Jersey: Princeton University Press, 2015.
- Stein, George J. 'Total Defense: A Comparative Overview of the Security Policies of Switzerland and Austria'. *Defense Analysis* 6, no. 1 (1990): 17–33.
- Stein, Janice Gross. 'Deterrence and Compellence in the Gulf, 1990-91: A Failed or Impossible Task?' *International Security* 17, no. 2 (Fall 1992): 147–79.

Stone, John. 'Conventional Deterrence and the Challenge of Credibility'. *Contemporary Security Policy* 33, no. 1 (2012): 108–23.

Stringer, Kevin D. 'Building a Stay-Behind Resistance Organization: The Case of Cold War Switzerland Against the Soviet Union'. *JFQ* 85 2nd Quarter (2017): 109–14.

## ENDNOTES

1. Erling Bjøl, *The Analysis of Small Power Politics* (Shou and Bruntland, 1971), 29.
2. Bjøl, *The Analysis of Small Power Politics*, 29.
3. Ang Cheng Guan, 'Singapore's Conception of Security', in *Perspectives on the Security of Singapore: The First 50 Years* (Singapore: World Scientific, 2016), 11.
4. Ang, 'Singapore's Conception of Security', 11.
5. Ang, 'Singapore's Conception of Security', 11.
6. John Mearsheimer, *Conventional Deterrence*, Cornell Studies in Security Affairs (Ithaca: Cornell University Press, 1983), 59.
7. Mearsheimer, *Conventional Deterrence*, 59.
8. Glenn Herald Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, New Jersey: Princeton University Press, 2015), 3, 9; Robert P Haffa Jr, 'The Future of Conventional Deterrence: Strategies for Great Power Competition', (*Strategic Studies Quarterly*, Winter 2018), 96.
9. John Stone, 'Conventional Deterrence and the Challenge of Credibility.' (*Contemporary Security Policy* 33, no. 1, 2012), 109; Haffa Jr, 'Future of Conventional Deterrence', 96.
10. Michael J. Mazarr, 'Understanding Deterrence', Perspective (RAND Corporation, 2018), 2.
11. Ian Bowers, 'IFS Insights 9/2018: Small State Deterrence in the Contemporary World' (*Norwegian Institute for Defence Studies*, 2018), 2.
12. Mazarr, 'Understanding Deterrence', 2.
13. Mazarr, 'Understanding Deterrence', 2.
14. Kam Kai Qing, 'The Viability of Deterrence Strategies for Non-Nuclear States', (*POINTER, Journal of the Singapore Armed Forces* 44, no. 1, 2018), 14.
15. Kam, 'Viability of Deterrence Strategies for Non-Nuclear States', 14.
16. Kam, 'Viability of Deterrence Strategies for Non-Nuclear States', 13.
17. Kam, 'Viability of Deterrence Strategies for Non-Nuclear States', 13.
18. Kam, 'Viability of Deterrence Strategies for Non-Nuclear States', 13; Li Huat Lee, 'Will Strengthening the SAF Mean Strengthening Singapore's Deterrence as a Non-Nuclear State?.'(*POINTER, Journal of the Singapore Armed Forces* 41, no. 4, 2015), 24.
19. Kam, 'Viability of Deterrence Strategies for Non-Nuclear States', 13.
20. Dmitry (Dima) Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force.'(*Security Studies* 26, no. 1, 2017), 165.
21. Michael Raska, 'Creating Reverse Asymmetry: Patterns of IDF's Military Innovation', RSIS Commentaries (S.Rajaratnam School of International Studies, 5 December 2012).
22. Raska, 'Creating Reverse Asymmetry'.
23. Avner Golov, 'Israeli Deterrence in the 21st Century' (*Tel Aviv: Institute for National Security Studies*, June 2016), 93.
24. Efraim Inbar and Shmuel Sandler, 'Israel's Deterrence Strategy Revisited.'(*Security Studies* 3, no. 2, 1993), 332.

25. Inbar and Sandler, 'Israel's Deterrence Strategy Revisited'.
26. Inbar and Sandler, 'Israel's Deterrence Strategy Revisited'.
27. Shmuel Bar, 'Israeli Strategic Deterrence Doctrine and Practice', (*Comparative Strategy* 39, no. 4, 2020), 329.
28. Adamsky, 'From Israel with Deterrence', 163.
29. Bar, 'Israeli Strategic Deterrence Doctrine and Practice', 330-331.
30. Adamsky, 'From Israel with Deterrence', 163.
31. Adamsky, 'From Israel with Deterrence', 166.
32. George J. Stein, 'Total Defense: A Comparative Overview of the Security Policies of Switzerland and Austria.' (*Defense Analysis* 6, no. 1, 1990), 19.
33. Stein, 'Total Defense', 18.
34. Stein, 'Total Defense', 21.
35. Stein, 'Total Defense', 21.
36. Dietrich Fischer, 'Invulnerability without Threat: The Swiss Concept of General Defense.' (*Journal of Peace Research* 19, no. 3, 1982), 216-217.
37. Stein, 'Total Defense', 21.
38. Stein, 'Total Defense', 20.
39. Stein, 'Total Defense', 19.
40. Stein, 'Total Defense', 19.
41. Fischer, 'Invulnerability without Threat', 216.
42. Stein, 'Total Defense', 24.
43. Kevin D. Stringer, 'Building a Stay-Behind Resistance Organization: The Case of Cold War Switzerland Against the Soviet Union.' (*JFQ* 85 2nd Quarter, 2017), 111.
44. Rolf Folland, 'Arctic Security: Deterrence and Détente in the High North.' (*The Arctic Institute*, 30 March 2021), <https://www.thearcticinstitute.org/arctic-security-deterrence-detente-high-north/>.
45. James Black et al., 'Enhancing Deterrence and Defence on NATO's Northern Flank' (*Santa Monica, Calif: RAND Corporation*, 2020), 32.
46. Black et al., 'Enhancing Deterrence and Defence on NATO's Northern Flank', 24-25.
47. Black et al., 'Enhancing Deterrence and Defence on NATO's Northern Flank', 35-36
48. Thomas Nilsen, 'Norway to Host Biggest Exercise inside Arctic Circle since Cold War.' (*The Barents Observer*, 14 April 2021).
49. Folland, 'Arctic Security'.
50. Justyna Gotkowska, 'Norway and the Bear: Norwegian Defence Policy - Lessons for the Baltic Sea Region', Point of View (*Warsaw, Poland: Ośrodek Studiów Wschodnich*, January 2014), 37-38.
51. Black et al., 'Enhancing Deterrence and Defence on NATO's Northern Flank', 8.
52. Janice Gross Stein, 'Deterrence and Compellence in the Gulf, 1990-91: A Failed or Impossible Task?' (*International Security* 17, no. 2, 1992), 147.
53. Stein, 'Deterrence and Compellence in the Gulf', 150-153.
54. Richard J. Harknett, 'The Logic of Conventional Deterrence and the End of the Cold War.' (*Security Studies* 4, no. 1, 1994), 88-89.
55. Harknett, 'The Logic of Conventional Deterrence and the End of the Cold War', 89.

56. Harknett, 'The Logic of Conventional Deterrence and the End of the Cold War', 98.
57. Moni Chorev, 'Surprise Attack. The Case of the Yom-Kippur War' (*Washington, DC: National Defence University*, 1996), 10.
58. Chorev, 'Surprise Attack. The Case of the Yom-Kippur War', 12.
59. Kam, 'Viability of Deterrence Strategies for Non-Nuclear States', 13.
60. Bowers, 'IFS Insights 9/2018', 2.



**ME5 Lim Sher Hern** is currently the Commanding Officer of Air Photo Unit. He was a Distinguished Graduate of the 52<sup>nd</sup> Command and Staff Course at the Goh Keng Swee Command and Staff College in 2021, and has a Master of Arts in Intelligence and International Security from King's College London. ME5 Lim is a Senior Military Intelligence Expert by vocation, and has served his previous command and staff appointments in SAF C4I.

# CYBER POWER – AN EXPERIMENTAL FRAMEWORK

By MAJ Alex Hoh Li Wei

## ABSTRACT

Cyber is the fifth domain after Air, Land, Sea and Space. It is evolving and contested by economic, security and civil interests. Dynamism in cyber must be matched with dexterity in policy and decision-making. However, many leaders remained unfamiliar with this domain. Consequently, responses may fail to address root-causes, exacerbate volatility, generating unexpected emergences in the complex and interconnected cyber domain. This essay suggests a framework for cyber power. The author exemplifies the application of this framework to operationalise threat-intelligence. He then explores gaps across issues relating to threat appreciation in cyberspace. Changes happen daily in this domain and the framework is not definitive.

Keywords: *Cyber; Cyberspace; Cyber power; National Security; Grey zone*

*The single biggest existential threat that's out there, I think, is cyber.*

*Michael Mullen<sup>1</sup>*

## INTRODUCTION

The fifth domain was labelled a 'grey-zone' for great power rivalry.<sup>2</sup> Fears of cyber-related actions, such as influence operations in the United States (US) Presidential Elections, as well as past attacks against Estonia, Georgia and Ukraine, have spurred countries to invest into enhancing their cyber capabilities. Consequently, some militaries have acquired defensive capabilities, as well as techniques and procedures for offensive cyber. Determinants of cyber power transcend mere facility in selecting and applying tools for different situations. Concomitantly, how cyber power is exercised follows a particular logic, considered through the assessed intent of potential actors, assessed levels of cyber capabilities, and circumstances of the situation at hand. This essay seeks to explain this dynamic from a national security perspective. It proposes a framework for threat analysis and response, and explores gaps in strategic appreciation across the cyber domain.

## SCOPE

The essay is broadly divided into three parts. It first discusses the domain of cyber and defines key terms within. It then examines how cyber power is used in relation to a framework to better understand its operational application. Finally, it explores security

trends and situates cyber with related issues in parallel. As a caveat, there is extant literature on this subject. The author's intent is not to overturn existing scholarship or mainstream discourses. Instead, he aims to read the issues with lenses of a planner, annotating sources and methodologies that he finds useful, and present related aspects of the topic in an accessible manner. The author hopes that more officers become interested in this domain, and in turn, will invest time and intellect to enhance planning for the future.

## CYBER BEGINNINGS

This section explores the landscape of cyber, specifically to understand how terms are derived and used. Etymological examinations allow the capture of the essence of the subject and gain insights into literal applications. The author discusses how the term 'cyber' originates. In the late 1940s, a field in biology and engineering studied communication and control systems in living beings and machines. This was 'cybernetics'. The root was Greek—*kubernētēs* (steersman), from *kubernan*—meaning 'to steer'.<sup>3</sup> Cybernetics was crucial to research into computer science and bio-mechanics. The concept went mainstream in the 1960s, with the term 'cyborg' (shortened from 'cybernetic organism'), which described man-machine entities. Against a backdrop of nuclear tensions in the Cold War, cybernetic imageries entered popular imagination. Cyborgs were portrayed as an evolutionary

step of mankind, repopulating a post-apocalyptic Earth devastated by atomics.

The use of ‘cyber’ in the modern context was only in 1982, when William Gibson coined ‘cyberspace’ in his science-fiction short story ‘Burning Chrome’. According to the Oxford English Dictionary (OED), it is ‘the notional environment in which communication over computer networks occurs’. While this sufficed initially, limitations soon became apparent in modern Internet interactions. The ubiquity of the Internet meant that cyberspace is less ‘notional’. Effects from the proliferation of personal digital devices also brought a convergence of social and informational, of cognition and identifications of self. This entails multifaceted definitions that better explicate nuances in cyberspace.<sup>4</sup>

Let us take a detour into a cyberspace environment we are more familiar with—the Internet. What we commonly refer to as ‘Internet’ is just one level of cyberspace. This ‘Surface Web’ is indexed by search engines and accessed by normal browsers. It comprises 5% of the whole Internet. The rest is ‘Deep and Dark Web’. The former is non-indexed and screened from web crawlers. These include credential-protected sites, such as emails or financial records, as well as unlinked content. Dark Web, on the other hand, is part of the Deep Web, hidden and accessible only by special browsers.<sup>5</sup> Activities on the Dark Web are often questionable. Illegal items are hawked on dark-marketplaces and transacted in cryptocurrencies to avoid detection.<sup>6</sup> The more ‘specialised’ ones may require invitations, members to vouch for you, or some ‘proof of work’ (illegal), before admission. The Dark Web is also a favoured staging area for co-ordinating cyber-attacks and where depositories of botnet armies are formed. It is an opaque and complicated space.

It is more complicated when we examine ‘cyber’ as a stand-alone. The OED defines ‘cyber’ as an adjective ‘relating to or characteristic of the culture of computers, information technology, and virtual reality’. It is used as a prefix to describe or form words relating to Information Technology (IT) and computers. However, practitioners will discover that ‘cyber’ is also a noun in selected fields of application. This form of use is inherent in this essay. Beyond explaining it as an evolving term, the larger implication is, how words are used indicate lines of thought, which in turn, influence

the creation of modes of understanding and operations.<sup>7</sup> Despite present difficulties in defining certain core terms, it is useful to have a working definition for cyber planning and appreciation.

Hence, one posits that ‘cyber’ in security analysis, refers to ‘information control expertise enabled by electronic and info-communication technology in a networked architecture’.<sup>8</sup> First, this ‘information control expertise’ refers, non-exhaustively, to an ability to manoeuvre, exploit, control, gain or deny access to, and mask or manipulate information. This is predicated on ‘electronic and info-communication technology’, which includes computerised and electronic modes of technology that transmit or facilitate the exchange of information. Finally, ‘networked architecture’ delineates the spatial and organisational elements of cyber. This is defined through *physical* (‘hardware’—locations, nodes, servers), *logical* (‘software’—hosting, web-data retrieval), and *neural-cognitive* (‘heart-ware’—meta-physical; identity and self).



The headquarters of Government Communication Headquarters in 2017.

## MEASURING CYBER POWER

How do analysts measure cyber power? Ralph Langer, of the Stuxnet malware fame, defined cyber power as ‘a society’s organised ability to leverage digital technology for surveillance, exploitation, subversion, and coercion in international conflict’.<sup>9</sup> While useful to understand application, power transcends mere ability in leveraging tools. Cyber may also be exercised beyond the prism of conflict. Jeremy Fleming, Director of the Government Communications Headquarters (GCHQ), gave a state-centric, outcome-based perspective, when he opined that ‘Cyber Powers’ are nations that possessed the ability to ‘direct or influence the

behaviour of others in Cyber space.<sup>10</sup> Hence, it is an instrument of the State, potentially exercised across the conflict continuum.<sup>11</sup>

Generating cyber power will require extensive ‘hardware’ and ‘software’. When we overlay the social and media dimensions, it becomes an avenue to affect the ‘heart-ware’ of the people. Given its interconnectedness with other operational dimensions, cyber remains inextricably linked and arguably dependent on the air, land and sea operational domains. The base to generate this power depends on ‘a set of resources that relate to the creation, control and communication of electronic and computer-based information infrastructure, networks, software, [and] human skills’.<sup>12</sup>

**Hence, one posits that ‘cyber’ in security analysis, refers to ‘information control expertise enabled by electronic and info-communication technology in a networked architecture’.**

It is more than just an organised ability to manipulate levers in the digital domain. Hence, when Langer described ‘a society can jump-start noteworthy cyber power without the corresponding capabilities in their civilian economy’, he was more accurately stating that states may acquire and operate an extensive cyber arsenal, without the corresponding means to sustain or project this power over a sustained period of time.<sup>13</sup> As he qualified subsequently, ‘organised capability required to sustainably project cyber power is extensive... [including] an infrastructure with command and control servers; a workforce of software developers capable of developing exploits and destructive code sequences; and big data analytics to process... terabytes of exfiltrated data’.<sup>14</sup> Therefore, when planners analyse state-centric cyber power, models should account for cyber in a ‘full-power’ sense. This should include the intent to use this power ‘in extremis... to disrupt, deny or degrade’ adversaries when threatened.<sup>15</sup>

Presently, a commonly-cited model is the Booz Allen Hamilton (BAH) Cyber Power Index. It uses 39 indicators focusing on four dimensions: legal and regulatory framework; social-economic context; technology infrastructure; and industry application. The original study comprises 19 countries from the Group of 20 (G20)—less the European Union.<sup>16</sup> Military power was conspicuous in its absence. The BAH index could be improved by adding defence cyber indicators. However, Intent is less clearly defined in the BAH Index. An alternative is the ‘Cline formula for national power’ as explained below:<sup>17</sup>

<b>Pp = (C+E+M) x (S+W)</b>	
Pp	- Perceived Power
C	- Critical Mass (Population and Territory)
E	- Economic Capabilities
M	- Military Capabilities
S	- Strategy
W	- Will

The former set (C+E+M) relates to quantifiable attributes of a nation-state, but conditioned by the latter set (S+W), which measures its perceived willingness to exercise the capabilities.<sup>18</sup> Elements in the equation require values to be ascribed to them. Evaluations via quantitative metrics are suitable for ‘hard’ criteria such as population and military assets. Qualitative analysis is more useful for ‘soft’ dimensions like public awareness or the will to fight. Common ranking methods such as Analytic Hierarchy Process could then be used to organise and derive an eventual power value. Element definitions and methods are also not fixed. Main elements can recur into sub-elements. Different multi-criteria decision tools could also be used to rank and calculate a power value. Adapting this for cyber would require adjustments. A revised Cline formula for cyber is proposed for use in this essay:

<b>PpCy = (C+E+M) x (S+W)</b>	
PpCy	- Perceived Cyber Power
C	- Critical Mass (education clusters; cyber groups) <sup>19</sup>
E	- Economic (cyber infra and technology; cyber workforce)
M	- Military (cyber command; # of cyber defenders)
S	- Strategy (national cyber strategy; legal & regulatory framework)
W	- Will (cyber awareness; susceptibility to cyber-crime) <sup>20</sup>

## ANALYSIS FRAMEWORK

So why is calculating cyber power useful? Calculating cyber power at the policy level allows planners to organise their cyber landscape more

coherently. It also gives planners a quick reference guide to 'who's-who' in the cyber domain, and helps sharpen their thinking when evaluating which criterion is relatively more important when measuring the cyber power of states. Thereafter, one could use the index to examine how cyber power is applied. The author has done that in this essay through a geostrategic reasoning framework. Using '**Intent; Capabilities; and Circumstances**' as the line of thought, planners may trace the exercise of cyber power by state actors, mapping the logical progression from assessed interests to observed actions. This framework may also be applied to non-state examples. However, actual determinants of cyber capabilities would require attenuation for different threat groups, proto-State or non-State actors.<sup>21</sup>

The logic behind 'Intent; Capabilities; and Circumstances' is as follows: Intent and Capabilities change slowly. The former is predicated on stakeholders who determine the expressed and (often) hidden interests of a state. This set of interests would remain fairly consistent and changes slowly over time. On rare occasions, changes may be abrupt if groups with different interests or calculus gained power, and thus, the ability to dictate fresh priorities and new objectives. Capabilities require time to build and are the slowest to change in a significant manner amongst the three. Substantial investments in time and material are also needed to build, operate and sustain capabilities over time. Cyber is no different. Tools may be quickly acquired off-the-shelf. However, the ability to wield them consistently, as well as evolve niche competencies, requires steady investments in time and effort. Circumstances are fastest to change, and usually exert a direct influence on intent, leading to changes over time.

## APPLICATION - CASE STUDY

Rendering strategic assessments into operational intelligence, (C+E+M) relates to Capabilities and (S+W) relates to Intent. Circumstances are read from global events and applied to 'Intent and Capabilities'. Thence, it is possible to predict the likelihood of cyber actions, depending on assessments—favourable or unfavourable—from 'Circumstances'. Numeric modifiers may be given to enrich the Cline cyber formula. 'Circumstances' are fluid, exerting an influence on stakeholder interests that govern 'Intent', thus leading

to changes over time. This dynamic can be expressed as an exponentiation on the base (S+W) set.<sup>22</sup> The resultant value allows the charting of any relative enhancements or erosions to the perceived cyber power, which provides an estimation of the opportunities or vulnerabilities to attacks. This revised Cline cyber-formula with modifier for the 'Circumstances' is as proposed:

$PpCy = (C+E+M) \times (S+W)^1$	
PpCy	- Perceived Cyber Power
C	- Critical Mass (education clusters; cyber groups)
E	- Economic (cyber infra and technology; cyber workforce)
M	- Military (cyber command; # of cyber defenders)
S	- Strategy (national cyber strategy; legal & regulatory framework)
W	- Will (cyber awareness; susceptibility to cyber-crime)
(Input) <sup>1</sup>	- Regional atmospherics; temporal incidents; natural events

This framework may be used to discern the logic behind attacks for identification and attribution. We can back-test on a known case-study to assess if our reasoning is sound and applicable for predictive and preventive early-warning.<sup>23</sup> On 23<sup>rd</sup> May, 2018, Cisco Talos reported that a sophisticated malware 'VPNFilter' was 'actively infecting Ukraine hosts at an alarming rate'.<sup>24</sup> The Security Service of Ukraine (SSU) warned that VPNFilter was a 'preparation for another Russian cyberattack aimed at destabilising the situation during the Champions League finals'.<sup>25</sup> They assessed that the 'mechanism of cyberattacks coincides with the techniques ... used in 2015-2016 during the BlackEnergy cyberattack'.<sup>26</sup>

## The nature of cyber favours anonymity.

Applying our framework, Russia had demonstrated prior **intent** to target Ukraine. Motives could be deduced from past incidents and even armed conflict, such as the annexation of Crimea. Cyber becomes another instrument of power by the Russian state to exert pressure and degrade the effective functioning of the government apparatus in Ukraine. This is probable as part of their assessed interests due to a continuing adversarial relationship.

When analysing **capabilities**, planners could compare past vectors, and examine codes, tactics, techniques and procedures. By observing attacks over a prolonged period, the investigators uncovered more clues. It showed that these attackers had a robust

infrastructure with skilled developers to develop exploits and destructive sequences to generate attack-evolutions leading up to VPNFilter. Such commitment and complexity is resource-intensive. It suggested that these attacks are beyond the finances of small groups or lone-wolf attackers. Hence, a state-sponsored group is most likely behind this attack.

## Increasingly, 'silent wars' with multi-channel actions across time and space look set to be the norm.

Finally, circumstances prior to first report (23<sup>rd</sup> May, 2018) and peaking at the Champions League finals (28<sup>th</sup> May, 2018) suggested that attacks were timed to create the most disruptions. This was linked to intent and similar to previous actions at major sporting events, for example, the cyber-attacks that disrupted the Pyeongchang Winter Olympics in 2018.<sup>27</sup> The Federal Bureau of Investigation (FBI), SSU and cybersecurity firms later confirmed that patterns and signatures showed that the attack was by a cyber-espionage group, APT28, also known as 'Sofacy' or 'Fancy Bear', with links to the Russian government.<sup>28</sup> Hence, the use of the 'Intent; Capabilities; Circumstances' framework yielded a possible actor, known techniques, and similar temporal vulnerabilities. Concomitantly, this framework draws out the motives, and linked them to means and timings behind the attacks. This is supported by the relative erosion of cyber power, resultant from the negative regional atmospherics and coincidence of a high-profile event.

Therefore, one surmised that the use of the cyber power measurement index allowed some degree of predictive analysis into the likelihood or vulnerability to attacks. In turn, this can help the analysts and planners to clarify their strategic threat landscape. Moreover, using the cyber power index in relation to 'Intent; Capabilities; Circumstances' narrows down probable actors based on interests and motivations. Concomitantly, this strategy-to-operation dynamic is matched against one's own cyber power. Hence, the strategic frame is checked against operational reasoning, which complements the technical aspects of

digital forensics, such as in analysing indicators of compromise.<sup>29</sup> Blending these inductive and deductive methods across strategic, operational and technical (tactical) dimensions reduces uncertainty and hastens responses by state agencies.

## LIMITATIONS AND FUTURE WORK

This framework is a rough-and-ready measure of cyber power and intent. It complements forensics to speed up identification of threats and attribution. More work can go into back-testing the method, as well as comparing it to other models for correlations or improvement. Nonetheless, cyberspace and the conduct of international relations remained opaque and near impossible to disentangle actual cause-and-effect. This is recognition that much of the cyber domain remains poorly explored. Consequently, the following sections juxtapose viewpoints against the cyber formula and strategic reasoning framework in this essay. The author hopes that an exploration of these gaps will engender future endeavours by military professionals and government practitioners along these lines.

### Cyber Deterrence

Can deterrence be exercised in the cyber domain? As seen from the VPNFilter case study, allegations may rest upon vague, circumstantial, and sometimes even anecdotal evidence. The nature of cyber favours anonymity. This often creates attributional problems, which relate to difficulties in identification of actors, and thus insufficient proof for political action. Similarly, such 'plausible deniability' over cyberspace allows state-actors to sponsor, launch or sustain cyber-attacks, yet conveniently distance themselves when exposed. Hence, does high ranking on the cyber power index confer immunity, or build hubris that draws nefarious elements to presage your fall? Given this situation, deterrence in the traditional sense—think mutual assured destruction—seems unlikely.<sup>30</sup> More research is needed to improve our understanding of cyber deterrence and to derive credible postures to forestall cyber-attacks. One likely area is Cold War dynamics, where deterrence and actions below the threshold of war persisted throughout the era of Superpower rivalry.

### Virtual Red Lines

Deterrence questions inevitably lead us to expressions of inviolable interests. States have 'red

lines', invisible or otherwise, which fixes the figurative points of no return, according to core interests. In cyber, which markers, when violated, justify government action? In a conventional sense, when physical infrastructure or territorial integrity is violated by identified opposing forces, there is arguably a legitimate cause for retaliation proportionate to the injury done. However, cyber attribution difficulties complicate timeliness and scope for responses. Moreover, causal relationship between cyber actions and physical reactions remains largely indirect. Nonetheless, examples such as the Stuxnet malware and the Shamoon wiper have shown that cyber weapons created to affect the controls of physical components have resulted in real-world destruction.<sup>31</sup> Use of cyber in this manner would increasingly generate tangible consequences. Hence, a need to respond may be inevitable if attacks lead to loss of lives, disruptions to essential services, and gratuitous destruction of critical infrastructure.

## Declaring Cyber War

There are difficulties in defining cyber conflicts, specifically, cyber war. When Russian forces attacked Georgia in 2008, a parallel attack was underway in the cyber realm. However, the composition of these forces was very different from those found in the physical domain. The latter were soldiers and airmen of the Russian state, while online forces could be anybody. Nationalistic Russians or busy-bodies from around the world may visit pro-Russia websites, download software, and conduct Distributed Denial of Service (DDoS) on Georgian sites. In this instance, such DDoS attacks could have emanated from a hodgepodge army of international cyber anarchists, pro-Russia citizens, or legitimate cyber forces. If states fight in cyber, does that mean that all operators are legitimate targets? It becomes more convoluted when nothing physical is happening. When Estonia shifted a Soviet war memorial in Tallinn in 2007, it precipitated a slew of cyber-attacks from Russia. There was no invasion but cyber-attacks disrupted essential services and even forced Estonia to disconnect from the Internet. Being such a connected nation, Estonia was especially affected. As states become more reliant on the Internet, the effects of cyber-attacks on governments and societies would increase in ways we have not yet begun to appreciate.<sup>32</sup>

## Confluence of Domains

The examples cited above cloud the question of what constitutes an act of war. Is a 'cyber war' possible without having a 'shooting war'? Perhaps the answer lies somewhere between. Increasingly, 'silent wars' with multi-channel actions across time and space look set to be the norm. Cyber disruptions are preceding, supporting, and disrupting military operations. Partnering means include 'polite men' organising themselves into 'self-defence groups' to aid people of disputed regions in 'peacekeeping actions'.<sup>33</sup> Citing self-determination, referendums are then organised to reflect the will of the populace, and to 'legitimise' transitions of sovereignty. 'Hybrid warfare' where the physical is conjoined with the logical, within the informational, and fought over narratives of history, is closer than we imagine<sup>34</sup>. Most of these are facilitated by cyber, propagated over the 'Internet of Things', tugging at the hearts and minds of audiences across the globe. Varying issues such as the veracity of events, legality of actions, and even the formation of social memories, are disputed and negotiated over the fifth domain.



*Kaspersky Virus Lab*

## Diffusion of Capabilities

As states continue to contest the narratives of history, the exponential growth of cyber technology and application is driven largely by private interests. In some ways, cyber power is no longer the exclusive purview of states or wielded from traditional organs of power. Multinational cyber-tech companies, like Google, Tencent Holdings, or Kaspersky Labs, may have more skilled personnel, tools and financial assets at their disposal than some national agencies. It remained unclear if the interests of corporations coincide with

that of their founders, needs of their host nations, or the profit imperatives of their shareholders. The revised Cline cyber-formula included cyber-tech companies under the aegis of a national cyber power. However, trust in corporations and their alignment with national interests remained an assumption.



*Former United States Navy Admiral Michael G. Mullen, 17<sup>th</sup> Chairman of the Joint Chiefs of Staff.*

## CONCLUSION

In this essay, the author explored the cyber domain and defined terms in cyber defence appreciation. Moreover, the author had revised the Cline formula to rank cyber power, which potentially

helps to clarify the threat landscape for predictive purposes. Concomitantly, this cyber ranking mechanism partners a strategic threat-analysis framework to ascertain the motives of potential adversaries, commensurate with capabilities, and corroborated with known facts. Complemented with operations- and technical-analysis, uncertainty is reduced and agencies could respond more decisively against the constant stream of cyber threats today.

However, as elaborated in this primer, the fragmented and evolving state of cyber does not fit easily into an all-encompassing model. Challenges might be best addressed concurrently, and at different levels, across strategic appreciation to operational application, as well as tactical dissections to technical indications. As we learn more about cyber, we begin to realise that many gaps still remained. Intelligence appreciation across cyber-related domains continues to be uneven. It is also increasingly unwise to perpetuate the military and civilian dichotomy in cyber, as threats and opportunities can easily emanate both ways. As Admiral Mike Mullen, then-Chairman of the Joint Chiefs of Staff, had posited, cyber, given unbridled growth and increasing confluence with hybrid-domains, could be the existential threat that herald the end of mankind. His caution is well advised. We need rules and a chance to build trust before our aggressive inclinations in cyber fulfil the promise that cyborgs had failed to deliver. However, the presence of danger is almost always matched with undiscovered opportunities. When digital transformation brings greater disruption, our agility in situation appreciation and decision-making, remains the surest way to enhance security and co-operation in the cyber domain.

## BIBLIOGRAPHY

- Baylis, J., Wirtz, J., and Gray, C. (ed.), *Strategy in the Contemporary World: An Introduction to Strategic Studies*, 4<sup>th</sup> Edition, Oxford University Press, 2013
- Caltagirone, S.; Pendergast, A.; Betz, C., 'The Diamond Model of Intrusion Analysis', *Defense Technical Information Center*, US Department of Defense, <http://www.dtic.mil/docs/citations/ADA586960>, (Accessed on: 27 May 2018)
- Checkland, P. and Scholes, J., *Soft systems methodology in action*, Chichester, Great Britain: John Wiley & Sons, 1990
- Cheong, Damien, (ed.), *Cybersecurity: Some Critical Insights and Perspectives*, RSIS, Nanyang Technological University, 01 Nov 2014
- Chivvis, Christopher, S., and Dion-Schwarz, Cynthia, 'Why It's So Hard to Stop a Cyberattack – and Even Harder to Fight Back', 30 Mar 2017, <https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html>, (Accessed on: 27 May 2018)
- Cimpanu, Catalin, 'FBI Takes Control of APT28's VPNFilter Botnet', 24 May 2018, *Bleeping Computer*, <https://www.bleepingcomputer.com/news/security/fbi-takes-control-of-apt28s-vpnfilter-botnet/>, (Accessed on: 27 May 2018)
- Cisco Talos, *New VPNFilter Malware Targets 500K networking devices worldwide*, 23 May 2018, <https://blog.talosintelligence.com/2018/05/VPNFilter.html>, (Accessed on: 28 May 2018)
- Cline, Ray, S., *The Power of Nations in the 1990s: A Strategic Assessment*, University Press of America, 2002
- Collins, Allan (ed.), *Contemporary Security Studies*, 3<sup>rd</sup> Edition, UK: Oxford University Press, 2013.
- Cowan, Gerrard, 'The Fifth Domain' in *Jane's Defence Weekly*, Vol. 55, Issue 23, 6 June 2018
- Cyber Security Agency of Singapore, *Singapore Cyber Landscape 2017*, ISBN: 978-981-11-7062-1
- Department of Defense, *The DOD Cyber Strategy*, Apr 2015 [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf), (Accessed on: 01 June 2018)
- Joint Publication 3-12, *Cyber Space Operations*, [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12R.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf), (Accessed on: 14 May 2018)
- Economist Intelligence Unit, *Cyber Power Index: Findings and Methodology*, Booz Allen Hamilton, 2011
- Estonian Foreign Intelligence Service, *International Security and Estonia 2018*, <https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf#page=57>
- Faisendier, A., *Systems Architecture and Design*, Belberaud, France: Sinergy'Com, 2012
- Falliere, N., 'Stuxnet Introduces the First Known Rootkit for Industrial Control Systems', *Symantec Connect*, <https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-root-kit-scada-devices>, (Accessed on: 27 May 2018)
- Fleming, J., Director GCHQ, *Fullerton Lecture*, International Institute for Strategic Studies, Singapore, 25 Feb 2019
- Forsberg, K., H. Mooz, et al., *Visualizing Project Management: Models and Frameworks for Mastering Complex Systems*, Hoboken, Wiley, 2005
- Fox, J., 'Propaganda, Art and War', in *War & Art: A Visual History of Modern Conflict* (ed.) J. Bourke, Realition Books: 2017
- Ginzburg, C., *Fear Reverence Terror: Five Essays in Political Iconography*, Seagull Books, 2017
- Hammes, Thomas, X., 'Technology Converges and Power Diffuses' in *Pointer*, Vol. 42 No. 4, 2016.
- Heinl, Cairtriona, 'The Role of the Military in Cyberspace: Civil-Military Relations and International Military Co-operation' in *Pointer*, Vol. 42 No. 4, 2016
- Hew, Strachan, *Carl von Clausewitz's On War – A Biography*, India: Manjul Publishing House, 2011
- Inkster, Michael, 'Why We Need to Measure Military Cyber Power', *World Economic Forum*, 29 Mar 2018, <https://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power/>

[www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power](http://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power), (Accessed on: 2 Apr 2018)

International Group of Experts, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017

International Group of Experts, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013

Kaplan, R., and Norton, D.P., *The Balanced Scorecard: Translating Strategy into Action*, Boston, MA: Harvard Business School Press, 1996.

Koh, Richard, 'Don't Let Cybersecurity to be an Afterthought', *The Business Times*, 18 July, 2018

Kompanichenko, Sergey, 'NATO Recon Missed Everything: Admiral Reveals Details of Crimea Operation', *Sputnik News*, 13 Mar 2015 <https://sputniknews.com/russia/201503131019448901/>, (Accessed on: 01 June 2018)

Kramer, Starr and Wentz (ed.) *Cyberpower and National Security*, University of Nebraska Press, 2009

Langer, Ralph, 'Cyber Power – An Emerging Factor in National and International Security', *Horizons: Journal of International Relations and Sustainable Development*, Autumn 2016, Issue No. 8, <https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security> (Accessed on: 01 June 2018)

Lockheed Martin, *The Cyber Kill Chain*, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>, (Accessed on: 4 July 2018)

Metzger, Max, 'InfoSec 2017: What Are Fancy Bears and Why It Matters, Even for SMEs', *SC Media*, <https://www.scmagazine.com/infosec-2017-what-are-fancy-bears-and-why-it-matters-even-for-smes/article/668094/>, (Accessed on: 27 May 2018)

Minárik, T., Alatalu, S., Biondi, S. Signoretti, M., Tolga, I., Visky, G., (Eds.), *2019 11<sup>th</sup> International Conference on Cyber Conflict: Silent Battle*, NATO CCDCOE Publications, 2019.

Morgan, Steve, '2017 Cybercrime Report: Cybercrime Damages Will Cost the World \$6 Trillion Annually by 2021', *Cybersecurity Ventures and Herjavec Group*, <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>, (Accessed on: 01 June 2018)

Nye, Joseph, S., *Cyber Power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010-----*The Future of Power*, NY: Public Affairs, 2011

Porche, Isaac, R., 'Getting Ready to Fight the Next (Cyber) War', *RAND Corporation*, 3 Mar 2018, <https://www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html>, (Accessed on: 01 June 2018)

Qiao, Liang, and Wang, Xiang Sui, *Unrestricted Warfare*, <http://www.cryptome.org/cuw.htm>, (Accessed on: 29 Jun 2018)

Qu, Yan Tao, 超限战: 作者新书发布: 首次披露美如何反超限战, Ministry of National Defense of the People's Republic of China, [http://www.mod.gov.cn/jmsd/2016-07/30/content\\_4704191.htm](http://www.mod.gov.cn/jmsd/2016-07/30/content_4704191.htm), (Accessed on: 29 Jun 2018)

Security Service of Ukraine, 'SBU warns of a possible large-scale cyberattack

on state structures and private companies ahead of Champions League Final', 23 May 2018, <https://ssu.gov.ua/ua/news/1/category/21/view/4823#.rzBG7GGw.dpbs>, (Accessed on: 28 May 2018)

Shevchenko, Vitaly, '“Little green men” or “Russian invaders”?', *BBC News*, 11 Mar 2014, <https://www.bbc.com/news/world-europe-26532154>, (Accessed on: 01 June 2018)

Starr, Stuart, H., *Towards an Evolving Theory of Cyberpower*, [https://ccdcoe.org/publications/virtualbattlefield/02\\_STARR\\_Cyberpower.pdf](https://ccdcoe.org/publications/virtualbattlefield/02_STARR_Cyberpower.pdf), (Accessed on: 14 May 2018)

Sutherland, Benjamin (ed.), 'Modern Warfare, Intelligence and Deterrence: The Technology that is Transforming Them', *The Economist*, UK: Profile Books, 2011

Symantec Security Response, 'The Shamoon Attacks', *Symantec Connect*, <https://www.symantec.com/connect/blogs/shamoon-attacks>, (Accessed on: 27 May 2018)

Taleb, Nassim, N., *The Black Swan: The Impact of the Highly Improbable*, US:Random House, 2007

The MITRE Corporation, *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)*, [https://attack.mitre.org/wiki/Main\\_Page](https://attack.mitre.org/wiki/Main_Page), (Accessed on: 23 Jul 2018)

Wack, Pierre, 'Scenarios: Uncharted Waters Ahead', *Harvard Business Review*, Sep-Oct, 1985

Walzer, Michael, *Just and Unjust Wars – A Moral Argument with Historical Illustrations*, 4<sup>th</sup> Edition, NY: Basic Books, 2006

Wee, C.H., *Sun Zi Art of War: An Illustrated Translation with Asian Perspective and Insights*, Singapore: Prentice Hall, 2003

Wingfield, N., Isaac, M., Benner, K., 'Google and Facebook Take Aim at Fake News', *The New York Times*, 14 Nov 2016, <https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html>, (Accessed on: 01 June 2018)

Van Vuureen, Jansen, and Leenen, L., 'A Model for Measuring Perceived Cyberpower' in *Proceedings of the 13<sup>th</sup> International Conference on Cyber Warfare and Security* (ed.) Hurley, J.S., and Chen, Jim Q., UK: Academic Conferences and Publishing International, 2018

Van Vuureen, Jansen, J.C et al. 'Building Blocks for National Cyberpower' in *Proceedings of the 11<sup>th</sup> International Conference on Cyber Warfare and Security* (ed.) Zlateva, T., and Greiman, V., UK: Academic Conferences and Publishing International, 2016

Zenko, Micah, 'The Existential Angst of America's Top Generals', *The FP Group*, 4 Aug, 2015, <https://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-generals-threat-inflation-islamic-state/>, (Accessed on: 01 June 2018)

## ENDNOTES

1. Zenko, Micah. 'The Existential Angst of America's Top Generals', The FP Group, 4 Aug 2015, <https://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-general-threat-inflation-islamic-state/>
2. Gen. Paul Nakasone, Commander, US Cyber Command, even noted that 'persistent engagement' was the go-to strategy to 'impose costs on the adversary in cyberspace' (Keynote speech, 9<sup>th</sup> Annual Billington Cybersecurity Summit, Sep 18).
3. Cyber, *Online Etymology Dictionary*, <https://www.etymonline.com/word/cyber>
4. Useful reading about cyber from a security perspective include Kramer, Starr and Wentz (ed.) *Cyberpower and National Security*; and Joint Publication 3-12, Cyber Space Operations, U.S. Department of Defense.
5. The Onion Router (TOR) is probably the most widely known of these special browsers.
6. A good example is the Silk Road (shut down by FBI in 2013). The currency of choice is usually bitcoin.
7. It sufficed to state here that definitions need to be situated in the proper context. How the author explains cyber is conditioned largely from cultural and organisation experience, and is by no means, universal.
8. This working definition by the author is used for illustrating concepts in this essay.
9. Langer, R., Cyber Power – An Emerging Factor in National and International Security, *Horizons: Journal of International Relations and Sustainable Development*, Autumn 2016, Issue No. 8.
10. Jeremy Fleming, Director GCHQ, Fullerton Lecture, International Institute for Strategic Studies, Singapore, 25 Feb 2019.
11. This essay is not specifically concerned about authority, legitimacy and proportionality in the context of *jus ad bellum* or *jus in bello*. The right to exercise cyber power by states is assumed.
12. Nye, J., *The Future of Power*, NY: Public Affairs, 2011.
13. Langer, 2016.
14. Ibid.
15. Jeremy Fleming, 2019.

16. Economist Intelligence Unit – Cyber Power Index: Findings and Methodology, Booz Allen Hamilton, 2011.
17. Cline, R., *The Power of Nations in the 1990s: A Strategic Assessment*, University of America Press, 1995.
18. A state with high quantifiable capabilities but lacks a coherent plan or will to use them, will cause their Pp to decline. Pp could even be 0, if S+W = 0. Conversely, a state with a lower level of capabilities, but demonstrates great will and organisational strategy, will boost its overall power due to a higher (S+W) modifier.
19. National population plays a big part in the cyber mass of a country. The number of groups in or aligned with a country is crucial because they may be rallied to a country's cause and boost cyber power.
20. The citizenry could be exploited for open-source intelligence collection or be compromised and become part of the enemy's botnet or denial of service attacks.
21. These should not include advanced persistent threats (APTs), which are usually state-sponsored and so named because they skilled, targeted, and persistent in their efforts.
22. The default exponential value is one (1), which indicates a normal, neutral or benign environment. A good situation should be given a +ve input, with more occurrences increasing the exponential. The inverse applies for bad situations, which incurs a -ve input, thus dividing the base S+W value.
23. For simplicity, perceived cyber power of Ukraine will not be calculated in the case-study. It is assumed that a hostile regional environment and hosting of a high-profile event contributed -ve inputs at the period in time.
24. Cisco Talos, 'New VPNFilter malware targets at least 500K networking devices worldwide, 23 May 2018, <https://blog.talosintelligence.com/2018/05/VPNFilter.html>
25. Security Service of Ukraine, 'SBU warns of a possible large-scale cyberattack on state structures and private companies ahead of Champions League Final', 23 May 2018, <https://ssu.gov.ua/ua/news/1/category/21/view/4823#.rzBG7GGw.dpbs>
26. Ibid.
27. Initial suspicion fell on the Lazarus Group, especially when Korean typography was found in initial analysis. Closer examination of codes and virtual private networks suggested that APT28 was the likelier attacker. Such attribution difficulties, exacerbated by false-flags, reinforced the need to quickly narrow down suspects.
28. Estonian Foreign Intelligence Service, 'Internal Security and Estonia 2018', <https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf#page=57>
29. Cyber practitioners may notice similarities with models such as 'Diamond Model of Intrusion Analysis' by Caltagiorne, Pendergast and Betz. However, 'Cyber Power Analysis' and 'Intent; Capabilities; Circumstances' is optimised for adversary-gaming and 'cyber-terrain' appreciation. It is more suitable for policy-planning and guidance of operational options. Concomitantly, tradecraft-centric models like 'Diamond Model', or platform - and lifecycle-models like 'Cyber Kill-Chain' (Lockheed Martin) and 'ATT&CK' (MITRE), are more suited for operational-planning and formulation of security (tactical) responses.
30. Deterrence by denial or by punishment might work. However, the ambiguity of cyberspace obfuscates risk-rewards.
31. Falliere, N., 'Stuxnet Introduces the First Known Rootkit for Industrial Control Systems', *Symantec Connect*, <https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-root-kit-scada-devices>  
The Shamoon Attacks', *Symantec Connect*, <https://www.symantec.com/connect/blogs/shamoon-attacks>
32. The Tallinn Manual and Tallinn Manual 2.0 are good start-points to explore this issue.
33. Shevchenko, Vitaly, "Little green men' or 'Russian Invaders", *BBC*, BBC Monitoring, 11 Mar 2014, <https://www.bbc.com/news/world-europe-26532154>
34. In 1999, Qiao Liang and Wang Xiang Sui, from the People's Liberation Army, proposed a similar concept in their book, 超限战 (warfare beyond boundaries) or 'Transfinite War' (official translation).



**MAJ Alex Hoh Li Wei** is currently a Branch Head in Defence Cyber Organisation. He is an Infantry Officer by vocation. MAJ Alex Hoh graduated from the 46<sup>th</sup> Command and Staff Course, Goh Keng Swee Command and Staff College, in 2016.

# APPLYING THE JUS AD BELLUM FRAMEWORK TO CYBERSPACE

By LTA(NS) John Yap & LTA(NS) Ryan Lee

## ABSTRACT

This essay outlines, and explores the challenges involved in, the application of the *jus ad bellum* framework to cyberspace. It seeks to address three central questions. How can norms of international law developed in a pre-cyber age govern cyberspace? When do cyber operations rise to the level of cyber warfare? When do cyber operations trigger the victim state's right to self-defence and what problems impede the exercise of that right?

*Keywords : Cyber; Jus Ad Bellum; Law; Use of Force; Self-defence*

## INTRODUCTION

On 6<sup>th</sup> May, 2019, the world saw its first openly-acknowledged kinetic military response to a cyber operation. The Israel Defence Force (IDF) allegedly detected the cyber operation during hostilities with the Palestinian militant group, Hamas. Attributing responsibility to human perpetrators operating from a compound in the Gaza Strip, the IDF launched an airstrike against it. The justification given was dubious: the airstrike was legitimate because the cyber operation was aimed at 'harming the quality of life of Israeli citizens'.<sup>1</sup>

Despite growing recognition of the threat posed by cyber operations to international peace, the development of cyberspace has outstripped the pace of development of international law.

Despite growing recognition of the threat posed by cyber operations to international peace, the development of cyberspace has outstripped the pace of development of international law. To date there is no binding international treaty governing cyber warfare and the unique characteristics of cyber operations continue to make the application of existing doctrines highly challenging and contentious.

Nonetheless, questions of international law pertaining to cyber warfare are of the utmost importance to Singapore. As a digital hub, the rule of law is vital to our national interest in preventing cyberspace from becoming a virtual Wild West. Understanding the challenges facing the law on cyber warfare allows Singapore to know its rights and obligations and work towards building a favourable international consensus. Moreover, understanding the state of the law on cyber warfare is necessary for the Singapore Armed Forces to formulate legitimate strategies to defend against cyber operations.

This essay seeks to provide an overview of some of the key challenges faced in accommodating cyber warfare within the doctrines of *jus ad bellum* (the corpus of international law governing states' decisions to commit acts of war). In this essay, 'cyberspace' refers to 'the environment formed by physical and non-physical components to store, modify and exchange data using computer networks.'<sup>2</sup> 'Cyber operation' refers to the 'employment of cyber capabilities to achieve objectives in or through cyberspace' and is used without prejudice to the legality of such operations.<sup>3</sup> 'Cyber warfare' is used in a non-technical sense to refer to cyber operations which engage *jus ad bellum* doctrines.

Three issues will be explored. The first concerns whether *jus ad bellum* doctrines, developed in a pre-cyber age, are applicable to cyberspace. The second concerns when it is that cyber operations rise to the level of cyber warfare; more precisely, when it is that cyber operations contravene the general prohibition on

the use of force. The third concerns the right of victim states to forcible self-defence—when is the right triggered and what are the challenges posed by the difficulty of attributing state responsibility for cyber operations. This essay concludes with a brief reflection on the implications of these debates to Singapore.

## EVOLUTION OF THE JUS AD BELLUM

It is trite that cyberwarfare is unlike conventional warfare in many respects. Warfare conventionally entails an attack by one state against another involving the violation of territorial integrity and the use of armed forces and kinetic weapons. In contrast, cyber warfare can be perpetrated through a non-spatial notional environment where information is both the weapon and the target. Cyber operations are diverse, with potential consequences falling along a spectrum spanning from mere inconvenience to devastating destruction. Their effects may be physical or non-physical, immediate or latent. They are perpetrated, not only by state organs, but non-state actors—some on behalf of their governments, others in pursuit of their own agendas. The unique characteristics of cyberspace can make the attribution of responsibility for cyber operations an arduous, if not impossible, task.

**Cyber warfare can be perpetrated through a non-spatial notional environment where information is both the weapon and the target.**

How can *jus ad bellum* doctrines govern cyber warfare, given that they were developed for conventional warfare and long predate cyberspace as we know it? To answer this question, a cursory understanding of the sources of international law is required. For present purposes, two sources must be distinguished: custom and treaties. Customary law is grounded in established state practice performed out of a sense of legal obligation, and is therefore, clearly capable of evolving with technological developments. Treaties, on the other hand, create binding legal obligations by virtue of the consent of signatory states.

However, just because treaties do not *explicitly* address the issue of cyber warfare, does not mean that

they are silent on the matter. This is established by the Vienna Convention on the Law of Treaties. Article 31(A) provides that ‘a treaty shall be interpreted in good faith... in the light of its object and purpose’, while Article 31(3)(b) provides that treaty norms are to be interpreted in the light of subsequent state practice applying the treaty. Where generic terms are used in treaties intended to be of continuing duration, the International Court of Justice (ICJ) in the *Navigational Rights* case held that those terms must be presumed to have an evolving meaning.<sup>4</sup>

Thus, we should expect existing *jus ad bellum* doctrines—whether derived from treaties or custom—to evolve over time. The real question, as François Delerue points out, must be: ‘is there anything preventing international law from applying to cyber activities?’<sup>5</sup> There is not. Unlike the expansion of warfare into the physical domains of air and space—where the necessity of specialised regimes is patent—cyberspace is but a *notional* environment spanning the physical domains. It is not in itself a separate ‘legal domain’.<sup>6</sup> Accordingly, cyber operations are caught by existing *jus ad bellum* doctrines, which ‘do not apply only to the forms of State activities existing at the time of their adoption or codification, but to State activities in general.’<sup>7</sup>

This is not to say that a specialised cyber treaty of sorts is not desirable. It merely means that the current absence of such a regime does not imply the absence of binding law. Thus, the remainder of this essay seeks to track—and outline the key debates surrounding—the evolution of *jus ad bellum* doctrines to accommodate cyberspace.

## THE USE OF CYBER FORCE

The fundamental question to ask, to determine if a cyber operation attributable to a state rises to the level of cyber warfare, is whether it amounts to a ‘use of force’? That is because there is a general prohibition on states’ use of force under customary and treaty law. The content of this prohibition is contained in Article 2(4) of the United Nations (UN) Charter, which provides that: ‘All members shall refrain in their international relations from the threat or use of force...’<sup>8</sup>

Important as the concept of ‘force’ is, it is never explicitly defined within the Charter. Historically, the

term has been understood as referring specifically to *armed* force. It was the use of weapons which, on this **instrument-based approach**, distinguishes uses of force from other forms of diplomatic, economic or political coercion. On this approach, the question of whether a cyber operation contravenes Article 2(4) of the Charter depends on whether it can be characterised and classified as akin to other traditional weapons.<sup>9</sup> However, the inadequacy of this approach has been much criticised. As Delerue observes, ‘most cyber operations would not qualify as use of force because they are difficult to characterise as armed or weaponised force... the similarity between cyber operations and traditional weapons... is very difficult to ascertain.’<sup>10</sup> The result would be under-inclusive, since even cyber operations with very physically destructive results may fail to meet the criterion.

In the light of this, two other approaches have been advanced. One of them is the **target-based approach**. According to it, a cyber operation amounts to a use of force if it is directed at national critical infrastructure (NCI).<sup>11</sup> However, this approach—on top of requiring a sharp break from orthodoxy—is over-inclusive. If left unqualified, it would mean that a cyber

operation which targets NCI is for that reason alone a use of force, irrespective of the severity of its consequences. This would, for instance, fail to distinguish cyber-kinetic attacks from merely information-gathering cyber exploitation. Furthermore, this approach would founder on the fact that there is no international consensus on what constitute NCI.<sup>12</sup>

The other is the **consequence-based approach**. On this approach, ‘it is not the instrument used that determines whether the use of force threshold has been crossed, but rather... the consequences of the operation and its surrounding circumstances.’<sup>13</sup> According to Michael Schmitt, the instrument-based criterion was only ever a ‘short-hand’ to ‘locate the point of demarcation’ between acceptable and unacceptable forms of coercion.<sup>14</sup> However, if it fails to ‘track the threats to shared values which... the international community would seek to deter’, then an approach focusing directly on the consequences and qualities of cyber operations should be preferred.<sup>15</sup> Alternatively, Marco Roscini attempts to reconcile the consequence-based and meaning of Article 2(4), weapons are ‘identified by their effects, not by the mechanism by which they produce destruction or damage.’<sup>16</sup>



*The Peace Palace in The Hague, Netherlands, seat of the International Court of Justice.*

The consequence-based approach has received considerable support and is currently ascendant. In the case of *Nicaragua v United States*, the ICJ held that the ‘scale and effect’ of certain hostile acts must be considered in determining whether they amounted to an ‘armed attack’.<sup>17</sup> Building on this, the Tallinn Manual 2.0 (which, although not binding, represents the opinion of its International Group of Experts on the state of international law) ‘found the focus on scale and effects to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not.’<sup>18</sup> Thus, Rule 69 of the manual provides that: ‘A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.’<sup>19</sup>

That said, the consequence-based approach can only provide very coarse-grained guidance as to whether a particular cyber operation meets the threshold for the use of force. Drawing on Schmitt’s work, the Tallinn Manual proposes eight factors as being relevant—the cyber operation’s severity, immediacy, directness, invasiveness, measurability of effects, military character, level of state involvement and presumptive lawfulness.<sup>20</sup> However, it concedes that these cannot serve as definitive legal criteria and that different states are likely to arrive at conflicting answers to the threshold question.<sup>21</sup>

While it is tolerably clear that a cyber operation which causes personal injury or physical damage constitutes a use of force, whether and when a cyber operation with severe but non-physical consequences constitutes a use of force is highly controversial. On the one hand, given the importance of cyberspace to modern society, it seems illogical to say that a cyber operation can *never* be a use of force in the absence of direct physical consequences.<sup>22</sup> On the other hand, a clear and stable standard to differentiate such cyber operations from highly disruptive forms of coercion that nonetheless fall short of the use of force (for example, economic sanctions) remains elusive.<sup>23</sup> Indeed, much of the debate is speculative as state practice is still very limited—to date, ‘no State or international organisation has ever publicly and unequivocally qualified a cyber operation as a use of force.’<sup>24</sup>

While it is tolerably clear that a cyber operation which causes personal injury or physical damage constitutes a use of force, whether and when a cyber operation with severe but non-physical consequences constitutes a use of force is highly controversial.

## THE RIGHT TO SELF-DEFENCE

A state’s right to use force in self-defence is enshrined in Article 51 of the Charter, which provides that: ‘Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations...’ There is no reason why, in principle, a cyber operation cannot trigger the victim state’s right to self-defence.<sup>25</sup> Moreover, where the right is triggered, a victim state’s response need not be confined to cyber operations (subject to the principles of necessity and proportionality).<sup>26</sup>

However, the picture is complicated by at least two factors.

### The ‘Armed Attack’ Trigger

The first complication is that not every use of cyber force contravening Article 2(4) of the Charter triggers the victim state’s right to forcible self-defence. According to Article 51 of the Charter, the right to self-defence is triggered by an ‘armed attack’. The prevailing view is that this term is not coextensive with the ‘use of force’, but a narrower sub-category of it.<sup>27</sup> As the ICJ held in the case of *Nicaragua v United States*, armed attacks are ‘the most grave forms of the use of force’, as distinguished by its ‘scale and effects’.<sup>28</sup> However, the precise parameters of these criteria are unsettled, there being some contrary indications that ‘[t]he gap between ‘use of force’ and ‘armed attack’ is not necessarily wide’.<sup>29</sup> In the *Oil Platforms* case, the ICJ declined to rule

out 'the possibility that the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'.<sup>30</sup> The lowering of the threshold for 'armed attack' has also been suggested by subsequent state practice.

The relevant question is thus how wide might the gap be between a use of cyber force and a cyber armed attack? In other words, what kinds of cyber operations would not trigger the victim state's right to forcible self-defence, despite being an unlawful use of force?

Again, the state of the law makes it difficult to say anything definitive, beyond providing illustrations of the broad principle. On one side of the line, the Tallinn Manual rules out 'acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services'.<sup>31</sup> On the other side of the line, it considers 'a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property' to clearly qualify.<sup>32</sup> From there, further details can be specified. A cyber operation targeting NCI is more likely to amount to an armed attack; a cyber operation with no physical consequences much less likely.<sup>33</sup> Multiple uses of cyber force can cumulatively rise to the level of an armed attack.<sup>34</sup>

Beyond these observations, however, consensus quickly evaporates. Thus, the Tallinn Manual notes that its International Group of Experts were split on whether the Stuxnet operation in 2010, which damaged Iranian nuclear centrifuges, rose to the level of an armed attack.<sup>35</sup> They were similarly split on the hypothetical scenario of 'a cyber incident directed against a major international stock exchange that causes the market to crash'.<sup>36</sup> The paucity of state practice and judicial decisions again means that these debates remain unresolved.

That said, a state that falls victim to the use of cyber force below the level of an armed attack is not defenceless. As the ICJ held in the case of *Nicaragua v United States*, a victim state in this position, may nonetheless, respond with non-forcible countermeasures.<sup>37</sup> These go beyond unfriendly but lawful retorsions, such as the expulsion of diplomats, cutting of aid, or restriction of access to cyber infrastructure within the victim state's territory.

Countermeasures are non-forcible 'measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation'.<sup>38</sup>



Anti-aircraft guns guarding Natanz Nuclear Facility.

Countermeasures may (but need not) take the form of cyber operations, as long as they comply with the requirements of customary law reflected in Part Three, Chapter II of the International Law Commission's (ILC) Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). Ordinarily, this includes the duty to give prior notice of the decision to take countermeasures and make an offer to negotiate.<sup>39</sup> However, the necessary element of surprise in cyber countermeasures means that they likely fall into the exception for 'urgent countermeasures' under Article 52 (2) ARSIWA.<sup>40</sup> Given the unlikelihood that (and uncertainty as to when) cyber operations trigger the right to self-defence, countermeasures are likely 'to be the primary form of self-help'.<sup>41</sup>

## The Problem of Attribution

The second complication impeding the exercise of the right to forcible self-defence is the difficulty of attributing state responsibility for cyber armed attacks. A victim state can only exercise its right to self-defence against another state if the latter is responsible for the initial cyber armed attack. This determination has two stages. The first involves identifying the human perpetrators of the cyber armed attack. This is a technical inquiry, which often requires first identifying

the machines used to launch the cyber armed attack. The second stage involves the application of legal standards to determine if the originating state is responsible for the cyber armed attack, and thus, a legitimate target of self-defence action.<sup>42</sup>

Each stage presents formidable challenges. In connection with the first stage, Nicholas Tsagourias observes that '[t]hree particular characteristics of cyberspace make attribution extremely difficult'.<sup>43</sup> Firstly, there is an abundance of technology enabling the perpetrators of cyber operations to remain anonymous. Secondly, cyber operations are often multi-stage—meaning that they are conducted through multiple infiltrated machines and computers across different states, concealing the perpetrators' identities. Thirdly, the rapid speed at which a cyber operation can materialise can overwhelm a victim state's forensic capabilities. All three of these characteristics were on display, for example, in the distributed denial of service operation against Estonia in 2007, involving a botnet of an estimated 85,000 computers spanning 178 countries.<sup>44</sup>

Given these difficulties, a question which arises is whether a victim state will itself be in breach of Article 2 (4) of the Charter if it exercises its putative right to self-defence on the basis of a good faith and reasonable factual error in attribution? This question is of crucial importance because decisions to take forcible self-defence action are necessarily time-sensitive and often made on the basis of incomplete information. This question, however, has given rise to two sharply conflicting views.

On one side of the debate, the ILC in its commentaries on ARSIWA provides that '[a] State which resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment'.<sup>45</sup> This, it holds, is equally applicable to self-defence.<sup>46</sup> Proponents of this position argue that it accords with the object and purpose of the Charter, which is to ensure that 'the right to unilaterally pursue the use of military force... is... limited as far as possible'.<sup>47</sup> As Henning Lahmann argues, '[i]f states were allowed to defend themselves

by forceful means even under ambiguity as regards [the authorship] of an armed attack... the risk of unpredictable escalation would vastly increase'.<sup>48</sup>

On the other side of the debate, the Tallinn Manual provides that 'the exercise of self-defence is... subject to the existence of a reasonable determination... as to the identity of the attacker... reasonableness will be assessed based upon the information available at the time they were made, not in light of information that subsequently becomes available'.<sup>49</sup> Proponents of this position argue that the object and purpose of Article 51 of the Charter is to provide a legal safeguard for states' inherent right to self-defence.<sup>50</sup> Since any decision to exercise the right to self-defence is necessarily self-assessed according to what is known at the time, such decisions—if reasonable and made in good faith—arguably satisfy international obligations, even if founded on a mistake.<sup>51</sup>

In connection with the second stage of the attribution inquiry, it is clear that cyber armed attacks perpetrated by state organs, or entities empowered by domestic law to perform state functions, are attributable to that state. Responsibility for cyber armed attacks can also be attributed to a state if the non-state perpetrators are *de facto* organs of that state, or are acting under its instructions, directions or control.<sup>52</sup> Whether the requisite relationship exists between that state and non-state actors is a question governed by a complex and inconsistent body of law, the elaboration of which is precluded by space.<sup>53</sup>

For present purposes, Delerue observes that three characteristics of cyberspace render the threshold set by existing attribution rules—based on the degree of state control—excessively high. Firstly, the decentralised nature of the internet means that cyber operations can be easily co-ordinated even with a very low level of organisation or overall control.<sup>54</sup> Secondly, 'cyber operations offer an easy means to act and to incentivise others to act'.<sup>55</sup> Thus, drawing any analogy between the situations where a state arms and trains private individuals, and where a state circulates ready-made malware to private individuals, is likely to be far-fetched and unhelpful.<sup>56</sup> Thirdly, the existing legal tests are extremely difficult to satisfy without the originating state's co-operation. That is because much of the

evidence needed to bridge the machine-human-state attribution gap will likely be located in the originating state. Thus, in the aftermath of the 2007 cyber operations against Estonia, Russia's refusal to co-operate ensured that no Russian human perpetrator was identified.<sup>57</sup>



Graphic illustrating the Safer Cyberspace Masterplan.

The recognition of these formidable problems has added fuel to a raging debate on whether the right to forcible self-defence can be invoked directly against non-state perpetrators of a cyber armed attack if the originating state is unable or unwilling to prevent or stop the attack. The traditional view is that an 'armed attack' under Article 51 of the Charter can only be carried out by another state. However, this view was challenged even before the 9/11 terrorist attacks.<sup>58</sup> In the aftermath of 9/11, military counterterrorism operations carried out by the United States (US) and its allies marked a significant shift in state practice in favour of the theory that the right to forcible self-defence can be directly invoked against non-state actors, irrespective of questions of state responsibility.<sup>59</sup>

The law on this issue remains unsettled. On the one hand, the ICJ has demonstrated its reluctance—in the two post-9/11 cases of *Wall Advisory Opinion* and

*Armed Activities*—to extend 'armed attack' to non-state actors directly.<sup>60</sup> On the other hand, such an extension is not expressly precluded by the language of Article 51 of the Charter and the law seems 'more than likely to evolve in this direction in the future.'<sup>61</sup> In line with the latter view, the majority of the Tallinn Manual's International Group of Experts were of the opinion that 'State practice has established a right of self-defence in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State.'<sup>62</sup> That said, while 'the extension of the right of self-defence to threats arising from non-state actors can be seductive in the cyber context', there is wisdom in Delerue's warning that 'this constitutes a very slippery slope and should be exercised with extreme caution.'<sup>63</sup>

## CONCLUSION

Singapore has, in recent years, paid increasing attention to cybersecurity. Since its establishment in 2015, the Cyber Security Agency has published several policy papers setting out Singapore's cybersecurity strategy.<sup>64</sup> These, as with the government's other official communications, have rightly emphasised the need to bolster passive cyber defence capabilities and strengthen the resilience of information infrastructure.

Beginning with an explanation of how pre-cyber norms of international law are evolving, this essay has outlined some of the key challenges involved in applying the *jus ad bellum* framework to cyberspace. Admittedly, the law is in an unsatisfactory state of flux—this essay barely scratches the surface. All the same, these debates are not ones that Singapore can sit on the fence. Should the situation arise, the questions they pose will demand answers. Much may depend on what answers Singapore is prepared to give. Accordingly, legal uncertainty calls for added engagement with the issues, not less. Understanding the law in this area, with all its imperfections, is crucial to Singapore's ability to set the parameters of its cyber defence strategy and build consensus on the world stage.

## ENDNOTES

1. E Borghard and J Schneider, 'Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal.' (10 May 2019) <<https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/>> accessed 21 July 2021.
2. M Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) ('Tallinn Manual'), Glossary, p 564.
3. *ibid.*
4. Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009, p. 213, [66]; see also Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14, [204].
5. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 13.
6. *ibid.*, pp 9-13.
7. *ibid.*, pp 13.
8. Article 2(4) (legal.un.org) [https://legal.un.org/repertory/art2/english/rep\\_supp7\\_vol1\\_art2\\_4.pdf](https://legal.un.org/repertory/art2/english/rep_supp7_vol1_art2_4.pdf)
9. M Gervais, 'Cyber Attacks and the Laws of War' (2012) 1 *Journal of Law & Cyberwarfare* 8, p 30.
10. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 289.
11. W Sharp, *Cyberspace and the Use of Force* (Aegis Research 1999), pp 129-32.
12. M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014), p 47.
13. Tallinn Manual, Commentary on Chapter 14, p 328.
14. M Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885, pp 913-914.
15. *ibid.*, p 914.
16. M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014), p 50.
17. *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14, [195].
18. Tallinn Manual, Commentary on Rule 69, p 331.
19. Tallinn Manual, Rule 69, p 330.
20. Tallinn Manual, Commentary on Rule 69, pp 334-336.
21. *ibid.*, pp 333-337.
22. F Delerue, *Cyber Operations and International Law* (CUP 2020)), p 298.
23. See for example J Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 *New York University Journal of International Law and Politics*, 57; M Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense' (2009) 32 *International & Comparative Law Review* 439; V Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places' (2005) 51 *Naval Law Review* 132.
24. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 342.
25. Tallinn Manual, Commentary on Rule 71, 340-341;  
M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014), p 71.
26. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 488.
27. Tallinn Manual, Commentary on Rule 71 341;

- F Delerue, *Cyber Operations and International Law* (CUP 2020), 327-328;
- M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014), p 72.
28. *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, [191].
29. Tallinn Manual, Commentary on Rule 71, p 341.
- M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014), p 72.
30. *Oil Platforms* (Islamic Republic of Iran v. United States of America), Judgment, I. C. J. Reports 2003, p. 161, [72].
31. Tallinn Manual, Commentary on Rule 71, p 341.
32. *ibid.*
33. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 304.
34. Tallinn Manual, Commentary on Rule 71, p 342.
35. *ibid.*, p 342.
36. *ibid.*, pp 342-343.
37. *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14, [249]. It has been suggested that forcible countermeasures short of armed attack may be taken in response to uses of force short of armed attack; however, this is a minority view.
38. International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the International Law Commission, 2001, Vol II, Part Two ('ARSIWA'), Commentary on Chapter II, p 128.
39. ARSIWA, Article 52(1)(b).
40. F Delerue, *Cyber Operations and International Law* (CUP 2020), pp 446-448.
41. *ibid.*, p 433.
42. *ibid.*, p 55.
43. N Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *Journal of Conflict & Security Law* 229, p 233.
44. *ibid.*
45. ARSIWA, Commentary on Article 49(1) ARSIWA, p 130.
46. *ibid.*
47. H Lahmann, *Unilateral Remedies to Cyber Operations* (CUP 2020), p 108.
48. *ibid.*
49. Tallinn Manual, Commentary on Rule 71, p 347.
50. H Lahmann, *Unilateral Remedies to Cyber Operations* (CUP 2020), p 100.
51. M Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1, p 77.
52. ARSIWA, Article 4.
- ARSIWA, Article 4; Article 5; Commentary to Article 5, p 43.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43, [391]-[412]; *Nicaragua v. United States* (n 16), [109]-[110]; *Armed Activities on the Territory of the Congo* (Democratic Republic of the

Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168. [160]; Prosecutor v. Dusko Tadić (Judgment) [1999] IT-94-1-A (ICTY, Appeals Chamber); ARSIWA, Article 8; ARSIWA, Commentary on Article 8, pp 47-49.

53. For a comprehensive discussion of such doctrines in the cyberspace context, see F Delerue (n 5), pp 118-144. See also H Lahmann (n 48), pp 87-97; Tallinn Manual, Rule 17 and Commentary, pp 94-100.
54. F Delerue (n 5), p 145.
55. *ibid.*
56. *ibid.*
57. *ibid.*, p 146.
58. See, for example, I Brownlie, 'International Law and the Activities of Armed Bands' (1958) 7 ICLQ 712.
59. H Lahmann, *Unilateral Remedies to Cyber Operations* (CUP 2020), pp 51-52.
60. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I. C. J. Reports 2004, p. 136, [139].  
*Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, I.C.J. Reports 2005, p. 168, [146].
61. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 464.
62. Tallinn Manual, Commentary on Rule 71, p 345.
63. F Delerue, *Cyber Operations and International Law* (CUP 2020), p 465.
64. Cyber Security Agency of Singapore, 'Singapore's Safer Cyberspace Masterplan 2020 (6 October 2020); 'Singapore's Operational Technology Cybersecurity Masterplan 2019' (1 October 2019); 'Singapore's Cybersecurity Strategy' (10 October 2016).



**LTA(NS) John Yap** graduated from the University of Oxford with a Bachelor of Arts in Jurisprudence (First Class), having read public international law. He served national service as an Air Defence Weapons Officer in 163 SQN. During active service, he was awarded the Full-time National Serviceman of the Year Award from the Air Defence and Operations Command and the Sword of Honour from the Officer Cadet School.



**LTA(NS) Ryan Lee** graduated from the University of Durham with a Bachelor of Laws. He served national service as an Air Defence Weapons Officer in 163 SQN and was awarded the RSAF Commander's Coin for his contribution to live operations.

# Instructions for Authors

## AIM & SCOPE

POINTER is the official journal of the Singapore Armed Forces. 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 GUIDELINES

POINTER accepts the contribution of journal articles 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 the following 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 and overseas training
- ⇒ Defence management, administration and organisational change issues
- ⇒ Defence technology
- ⇒ Warfighting and transformation
- ⇒ Leadership
- ⇒ Organisational Development
- ⇒ Conflict and Security Studies
- ⇒ Cyber Warfare / Cyber Security

### 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 and 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](mailto: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 completed the first time it is cited. Subsequent

references to the same source may be abbreviated.

The various formats of endnotes are summarised 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 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), issues 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.

### Article 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 the 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 2016,

<https://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/siteen0.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](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/authorsguid.html>.

### EDITORIAL ADDRESS

Editor, POINTER

AFPN 1451

500 Upper Jurong Road

Singapore 638364

Tel: 6799 7755

Fax: 6799 7071

Email: [pointer@defence.gov.sg](mailto:pointer@defence.gov.sg)

Web: [www.mindef.gov.sg/sahti/pointer](http://www.mindef.gov.sg/sahti/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 license:

- 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/requestform.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>

