# 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: C*yber; Cyberspace; Cyber power; National Security; Grey zone*

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

*Michael Mullen* [1]

## INTRODUCTION

The fifth domain was labelled a 'grey-zone' for great power rivalry.[2] 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'.[3] Cybernetics was crucial to research into computer science and bio-mechanics. The concept went main-stream 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.[4]

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.[5] Activities on the Dark Web are often questionable. Illegal items are hawked on dark-marketplaces and transacted in cryptocurrencies to avoid detection.[6] 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.[7] 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'.[8] 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'.[9] 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.'[10] Hence, it is an instrument of the State, potentially exercised across the conflict continuum.[11]

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'.[12]

**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.[13] 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'.[14] 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.[15]

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.[16] 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:[17]

**Pp = (C+E+M) x (S+W)**

| | | |
|---|---|---|
| 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.[18] Elements in the equation require values to be ascribed to them. Evaluations via quantitative metrics are suitable for 'hard' criterions 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:

**PpCy = (C+E+M) x (S+W)**

| | | |
|---|---|---|
| PpCy | - | Perceived Cyber Power |
| C | - | Critical Mass (education clusters; cyber groups)[19] |
| 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)[20] |

## 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.[21]

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.[22] 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:

$$PpCy = (C+E+M) \times (S+W)^{I}$$

| | | |
|---|---|---|
| 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) $^{I}$ | - | 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.[23] On 23rd May, 2018, Cisco Talos reported that a sophisticated malware 'VPNFilter' was 'actively infecting Ukraine hosts at an alarming rate'.[24] 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'.[25] They assessed that the 'mechanism of cyberattacks coincides with the techniques … used in 2015-2016 during the BlackEnergy cyberattack'.[26]

## 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 (23rd May, 2018) and peaking at the Champions League finals (28th 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 Pyeonchang Winter Olympics in 2018.[27] 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.[28] 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.[29] 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.[30] 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.[31] 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.[32]

## 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'.[33] 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[34]. 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, 17th 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*, 4th 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, Nayang 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*, 3rd 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, (Accessed on: 01 June 2018)

Joint Publication 3-12, *Cyber Space Operations*, 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, Caitríona, '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, (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 11th 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, (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, (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, (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*, 4th 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 13th 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 11th 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, 9th 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 46th Command and Staff Course, Goh Keng Swee Command and Staff College, in 2016.