Cyber Power – An Age of Perpetual Disruption

by **ME5 Calvin Seah Ser Thong**

Abstract:

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

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

INTRODUCTION

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

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 Some have even claimed that cyber power is making the Clausewitzean paradigm of war 'outdated' and 'ever more irrelevant'.[3] In 2011, the US DoD even recognised cyber space as an 'operational domain' in which its forces will be trained to respond to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

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

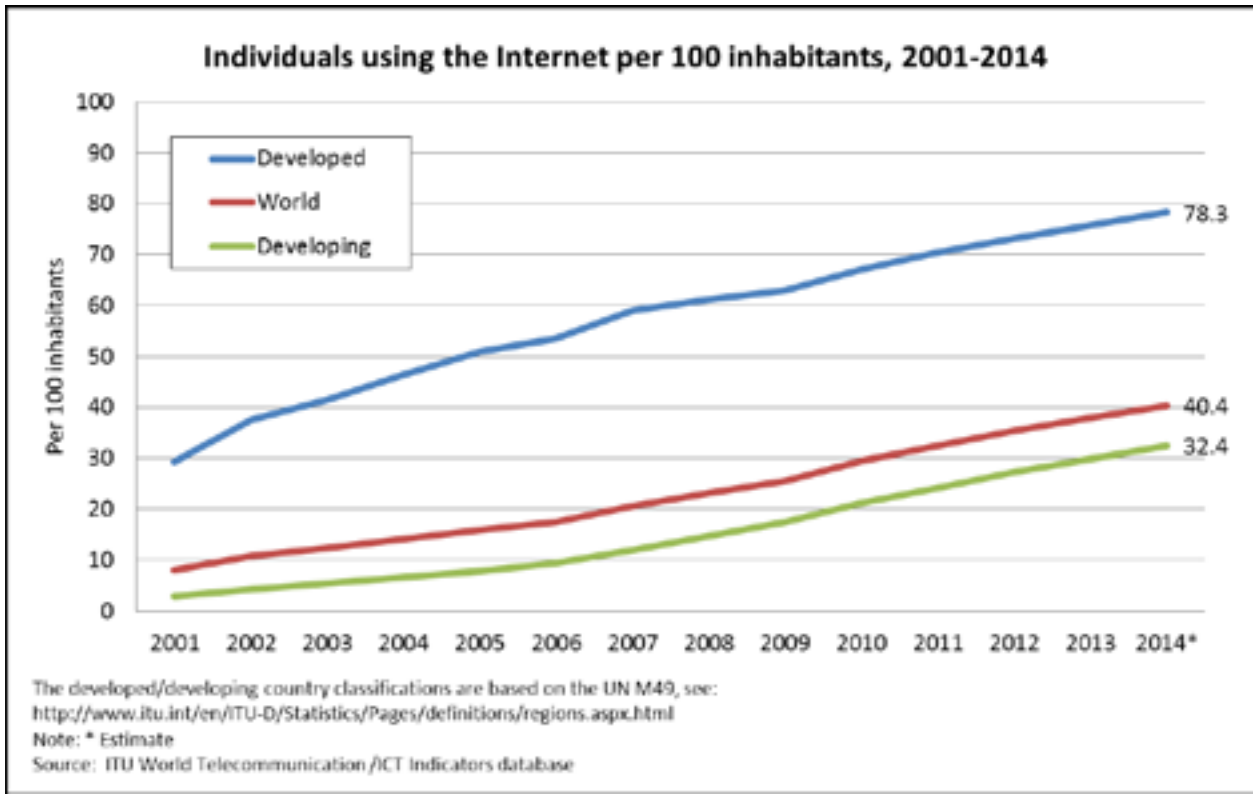

Figure 1: Internet users' continual growth[6]

THE DOMAIN OF CYBER SPACE

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

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

Figure 2. Interconnectivity of the Cyber Domain[11]

DEFINING CYBER POWER

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

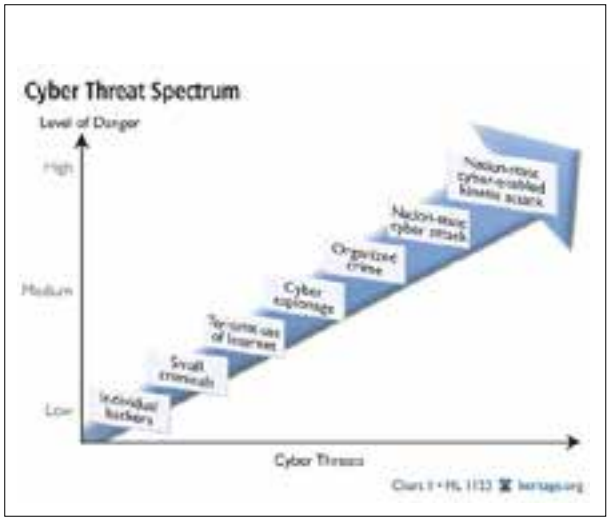

Figure 3: Cyber Threat Spectrum of the various threats and level of danger posed[14]

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

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

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

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

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

DEFINING PERPETUAL DISRUPTION THROUGH CYBER POWER

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

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

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

EXAMPLES OF CYBER THREATS

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

is 'boundary-less', thus increasing their attractiveness for the pursuit of political objectives.

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

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

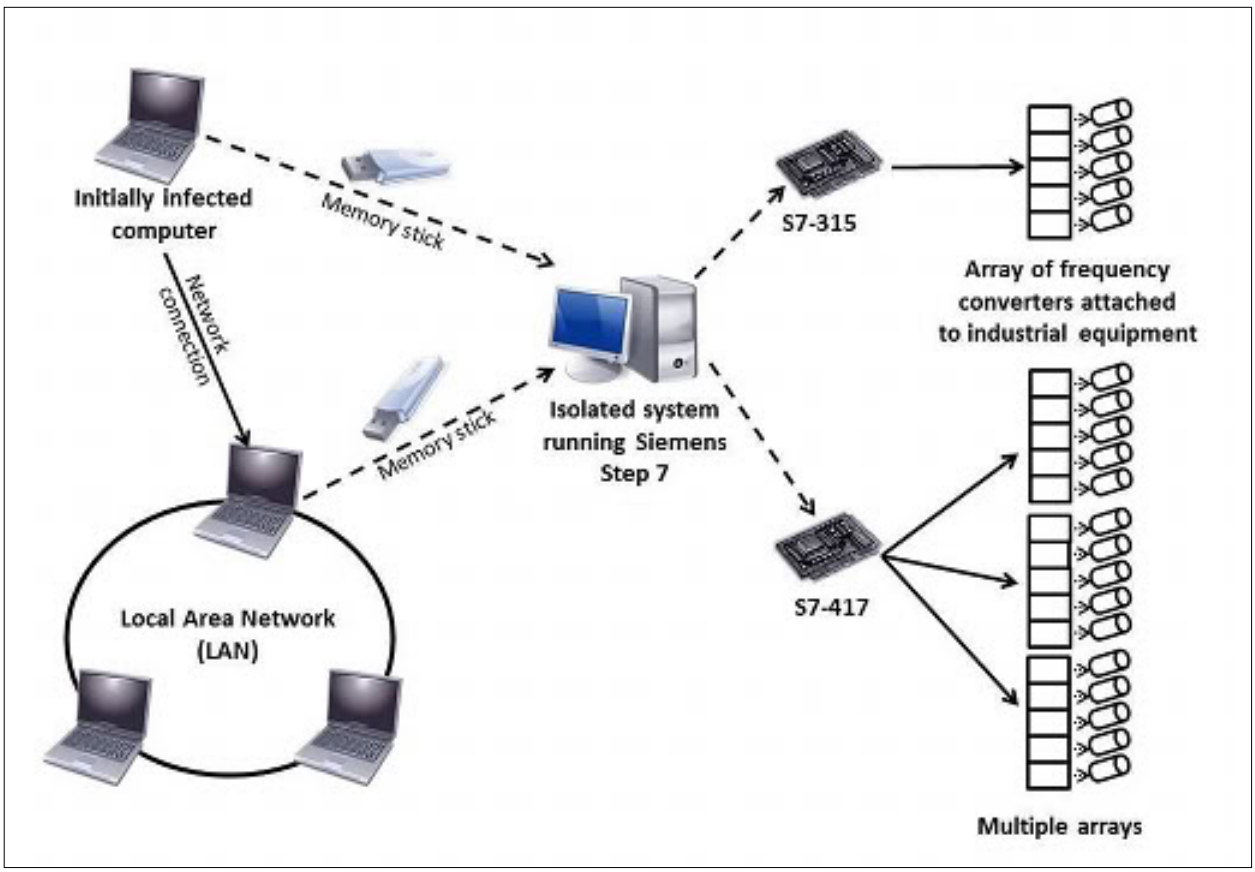

Figure 5: Propagation of the Stuxnet worm[29]

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

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

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

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

Figure 6: Actual profile of US Admiral James Stavridis.

Cyber Attack – Ukraine And Russia Cyber Conflict (2014)

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

WHY PERPETUAL DISRUPTION?

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

EFFECTS

Long Range and High Speed

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

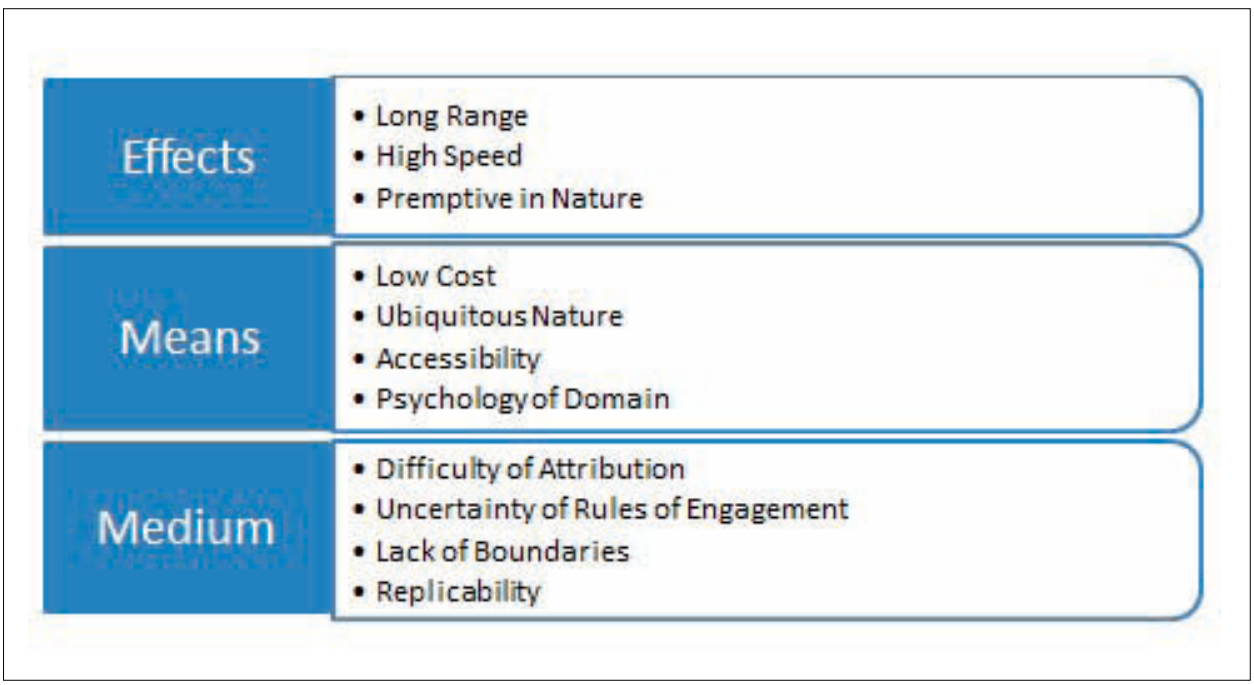

Figure 7: Factors resulting in Perpetual Disruption by cyber power

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

Pre-Emptive In Nature

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

MEANS

Low Cost

The cost of entry into the cyber domain is considerably low. Both the expertise and resources

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

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

Ubiquitous Nature

Cyber space is critical in the everyday functioning of not just the industrially-developed nations, but also the emerging and developing ones. This overwhelming reliance on cyber space throughout the modern society presents an attacker with an abundance of targets, thereby resulting in immense pressure on its successful defence. Cyber power is thus ubiquitous,

as it can enable the projection of air, land, sea, and space power as well as influence the four instruments of power represented in the DIME model. Our reliance on cyber space is ever increasing and it would be an easy means for the use of cyber power to potentially do damage to critical infrastructure.

Accessibility

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

Psychology Of Domain

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

MEDIUM

Difficulty Of Attribution

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

Uncertainty Of Rules Of Engagement

The rules of engagement of conventional warfare are clearly enshrined by the Geneva Convention and Article 51 of the UN Charter. However, these rules do not apply in cyber space which is boundless and borderless.[55] While the Pentagon has warned potential adversaries of the consequence of carrying cyber attacks against the US, there are uncertainties on what kind of cyber attacks would constitute a use of force.[56] There is currently no consensus on how regulations would be used to govern cyber conflicts as well as the thresholds for when a disrupting cyber

attack becomes a casus belli for a more traditional military response.[57] Furthermore, there is no effective international arrangement that performs law enforcement in cyber space. Given the international nature of many cyber threats, national enforcement efforts will be less effective than an integrated international effort.

Lack Of Boundaries

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

Replicability

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

AN AGE OF PERPETUAL DISRUPTION

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

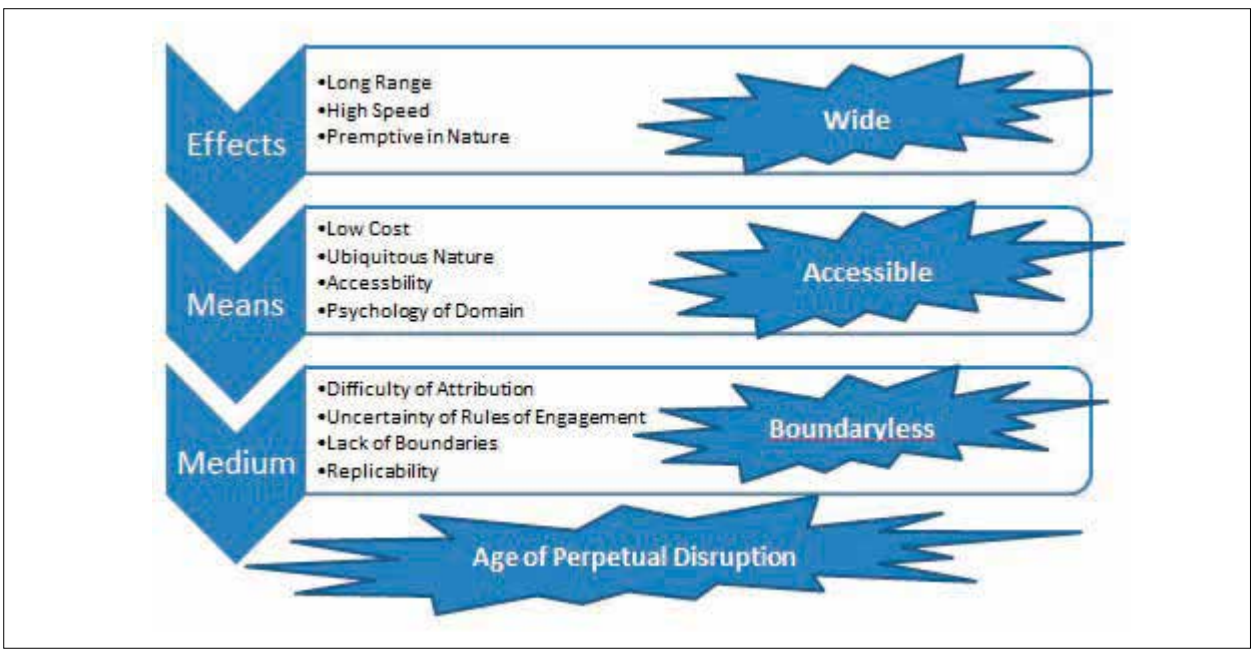

Figure 8: Factors culminating into Perpetual Disruption

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

CONCLUSION

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

ENDNOTES

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

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

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

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

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

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

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

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

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

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

27. The Economist, "War in the fifth domain."

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

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

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

30. Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

49. Joseph S. Nye Jr, Cyber Power.

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

51. Ibid.

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

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

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

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

56. Siobhan Gorman and Julian E. Barnes, "Cyber Combat : Act of War," The Wall Street Journal, 2011, http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

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

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

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

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

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