CYBERWAR – VIEWED THROUGH THE PRISM OF CLAUSEWITZIAN STRATEGY

Commodore Vishwanathan K Ganapathi, VSM

Introduction

In a globalised world where speed and reliability of information exchange is the *sine qua non* of technological advancement, the importance of cyberspace to a country is immeasurable. Knowledge and awareness, which derive from the degree to which cyberspace can be exploited for rapidly storing, manipulating and disseminating data, have become important measures of a nation's power.[1] As a consequence, the destruction or disruption of any of the constituent elements of cyberspace from a cyber attack would not just blunt a country's ability to gain strategic advantage from its technological superiority but would gravely threaten its security as well. Depending on their intensity and complexity, cyber attacks can inflict a wide spectrum of damage ranging from less dangerous depredations like the theft of personal information and digital heists to highly destructive actions like the disruption of critical infrastructure- 'the facilities, systems, sites and networks necessary for the delivery of essential services and functions'[2]- industrial sabotage, subversion, data destruction or theft of sensitive information. It is the latter category, most often believed to be orchestrated for political reasons by a potential adversary, which has transformed cyber attacks from being perceived as a trivial problem befitting address by an IT professional to one that merits the focus of policy planners and strategists alike.[3]

The concerns of governments about the gravity of the threat from cyber attacks stem from the certitude that easily accessible destructive technologies are being exploited by state and non-state actors alike to launch attacks even against powerful adversaries several thousand miles away. Episodic cases go so far as to suggest the increasing tendency of nations to employ them as an instrument of coercion in furtherance of policy objectives. Symantec's 2014 report paints a dismal picture: a majority of the global targeted attacks in 2013 were directed at

---

[1] *Sean Kay, Global Security in the 21st Century (USA : Rowman and Littlefield Publishers Inc, 2012), 175.*
[2] *UK Cabinet Office, "Sector Resilience Plans for Critical National Infrastructure 2010", accessed Dec 22, 2013, www.gov.uk/government/uploads/…/sector-resilience-plan.pdf.*
[3] *Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008), 41–65.*

governments and industrial sectors crucial to economic growth viz. manufacturing and mining. The odds of them being attacked were over 30%.[4] As a consequence, cyber attacks have been propelled to the forefront of national security strategy in many a country; a reality amply evidenced by the spate of recent legislations and executive orders that have made it obligatory for critical infrastructure providers to share with the government information on cyber attacks that their facilities experience.[5]

These fears, however, are not shared by everybody. While they do concede to cyberspace being a new domain of warfare, many scholars and security professionals decry the use of the term cyber war- the terms cyber attack and cyber war are often used interchangeably- as they doubt the ability of this instrument to independently achieve strategic or political objectives in the manner that conventional war in the other domains can. Arguing that only traditional war imbued with a violent character by virtue of its ability to deliver kinetic force can compel the enemy to do our will, they aver that cyber war, devoid of the ability to cause physical damage and corporeal harm, cannot coerce the enemy.[6] Strident claims about the likelihood of a 'Cyber Pearl Harbour,' 'Cyber 9/11' or 'Cyber Armageddon' are therefore dismissed as being alarmist and baseless.[7]

Notwithstanding sensational events in the recent past like the sabotage of a nuclear enrichment plant in Iran, frequent attempts to disrupt essential services in many countries, the theft of sensitive information worth billions of dollars from government and research laboratory networks, and the complete destruction of information databases of global companies–all of which smack of state-sponsored cyber attack campaigns with underlying political objectives- the debate rages on whether cyber attacks do by themselves threaten national security or simply serve as a metaphor to justify dark warnings. While the contention of critics may seem convincing at an intuitive level, it would be germane to evaluate the solidity of this disputation against logical inferences drawn from contemporary incidents.

---

[4]*Symantec Corporation, "2014 Internet Security Threat Report", accessed Aug 29, 2014, www.symantec.com.*

[5]*"To the Barricades- How America and Europe are trying to Bolster their Cyber-Defence," The Economist (London), February16, 2013, 46.*

[6]*Danny Steed, "Cyber Power and Strategy: So What?" Infinity Journal 2 (Spring 2011), 21-24.*

[7]*David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," Journal of Strategic Affairs, Vol.35, No. 5 (Oct 2012): 695.*

Strategic Strike

In November 2010, Iran's President Mahmoud Ahmedinijad conceded on state television that several centrifuges at the Natanz uranium enrichment facility had been affected by a software glitch and had to be replaced. The setback resulted in uranium enrichment at the plant being halted for several months.[8] The sabotage of nearly twenty percent of the centrifuges at the Natanz facility-the flagship of Iran's nuclear program - by the 'Stuxnet' worm over a period of nearly two years has raised the spectre of cyber attacks having evolved into a weapon of choice for strategic coercion. Certified by reputed anti-virus companies as a worm of unprecedented sophistication, 'Stuxnet' is believed to have been a product of design and intelligence collaboration between the United States and Israel to delay Iran's uranium enrichment programme by a few years.[9]

The optimism of cyber security professionals that Supervisory Control and Data Acquisition (SCADA) devices–computerised 'industrial control systems' that automate the industrial process through user programming and feedback from integral sensors[10] are reasonably secure from a cyber attack by virtue of their physical separation from the Internet and complex design was shattered when it was found that 'Stuxnet' successfully intruded into the isolated industrial control system at Natanz[11] and specifically targeted the heart of the enrichment process: the Siemens-designed Programmable Logic Controller (PLC) that regulates the speed of the centrifuges through frequency converters. This it did by modifying code on the PLC thereby altering its operating parameters and consequently the speed of the centrifuges, which, over a period of time, not only damaged the centrifuges but also resulted in incomplete uranium enrichment.[12] The PLC is normally programmed before embedding it in the industrial control system; a process that warrants its physical connection to a Windows computer known as a 'Field Programmable Gate' in industrial parlance.

---

[8] *Ladane Nasseri, "Ahmadinijad Confirms Several Iran Centrifuges Affected by Computer Virus," accessed January 24, 2013. www.bloomberg.com/news/2010-11-29.*

[9] *William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Crucial in Iran Nuclear Delay," New York Times (January 16, 2011): A1.*

[10] *Elihu Zimet and Edward Skoudis, "Graphical Introduction to Structural Elements of Cyberspace," in Cyberpower and National Security, ed Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (USA: NDU Press & Potomac, 2009), 94.*

[11] *POST Note 389, "Cyber Security in the UK," UK Parliamentary Office of Science and Technology (September 2011), 2.*

[12] *Kaspersky, "Kaspersky Lab Provides its Insights on Stuxnet Worm," Virus News, 24 September 2010, accessed 22 January 2013, www.kaspersky.com.*

Since the 'Field Programmable Gate' is never connected either to the Internet or a network for reasons of safety, it could have only been infected through portable media like a USB drive carrying the worm plugged in either carelessly or maliciously with insider assistance. 'Stuxnet,' therefore, successfully bridged the air gap, thus rendering tenuous the argument that systems that which do not connect to the Internet seldom risk being infected. Demonstrating a rare degree of complexity in executing only when it detected the specific Siemens designed PLC and its associated centrifuge cascade - a cluster of spinning centrifuges - that was unique to the Natanz facility, 'Stuxnet' was clearly a precision weapon designed to decapitate Natanz. Central to the worm's stealth and destructiveness was its ability to conceal rogue modifications it made to the PLC's operating parameters from the operators, as also the plant's safety mechanism, which would otherwise have shut down the centrifuges to prevent damage to them.[13]

As the archetypal industrial sabotage weapon, 'Stuxnet' set the bar at a very high level in terms of complexity by incorporating hitherto unseen features like multiple zero-day vulnerabilities (newly discovered bugs for which security patches are yet to be distributed) in Microsoft machines; automatic self-update by connecting to a remote command and control server if the infected machine or USB drive were to be inadvertently connected to the Internet; stolen digital certification to authenticate its driver files thereby evading detection; self replication through removable media and networks; gaining root (administrator) access to the computer; fingerprinting the PLC of the industrial control system to determine if it was indeed the desired target; and, deceiving the safety cut outs and operators into believing that the system was operating smoothly.[14]

Given the resources and time it must have taken to design a worm of this functional intricacy, it is obvious that 'Stuxnet' was the handiwork of a nation, or nations. Without government backing, it would hardly have been possible to write a 50 kilobyte source code with as many as four zero-day exploits capable of delivering a non-kinetic precision strike. Quite indisputably, the code developers would have needed access to proprietary information related to the PLC, the centrifuge cascade, as also the plant's safety mechanisms. More importantly, developing a worm of such precision would have necessitated intimate

[13] *Ivanka Barzashka, "Are Cyber-Weapons Effective," RUSI Journal, Vol. 158, No. 2 (April/May 2013): 49.*

[14] *Nicolas Falliere, Liam O Murchu and Eric Chien, "W32. 'Stuxnet' Dossier," Symantec Security Response (Feb 2011): 1-4.*

knowledge of the enrichment operations and the schematics of the 'industrial control system' in use at Natanz; awareness of exploitable software vulnerabilities in the system; access to the 'Field Programmable Gate' for a physical upload of the malware;[15] and, facilities to field test the malicious code in a mirror environment to the one obtaining at Natanz. It is quite possible that the Siemens technicians on-site colluded in the plot to infect the 'Field Programming Gate.'[16]

Did 'Stuxnet' Accomplish Political Objectives?

Imbued with a definite political objective, 'Olympic Games'- the codename for the 'Stuxnet' operation- thrust into the strategic realm a new form of national power capable of being exploited as an instrument of policy: cyber power derived from the ability to exploit cyberspace.[17] The argument that cyber power, barring an exceptional ability to gather copious volumes of intelligence, disrupt networks that underpin the enemy's hard power and critical infrastructure, and optimise one's own use of conventional military power, lacks the coercive ability required to achieve strategic objectives, was demonstrably challenged.[18] 'Stuxnet' may not have possessed the violence of a military strike but it was able to achieve what sanctions and the threat of force were unable to deliver: the forcible imposition of a temporal delay in the program's fruition, thereby giving stringent sanctions and international diplomacy more time to take effect.

Mossad's abrupt and unexplained revision of its estimate of Iran's likely possession of nuclear capability from 2012 to 2015 serves not just to corroborate this accomplishment but also confirms Israeli involvement in the sabotage.[19] Viewed from the perspective that Iran had material for only a limited number of centrifuges and therefore lacked the cushioning ability to absorb the attrition of approximately a thousand centrifuges, it would seem that 'Stuxnet' did indeed achieve what it was meant to. Sanctions further exacerbated Iran's bleak chances of sourcing replacement material owing to the vintage of the centrifuges at the Natanz enrichment facility. In essence, the strategic employment of cyber power

[15] *Dan Raviv and Yossi Melman, Spies Against Armageddon (New York: Levant Books, 2012), 12.*
[16] *Jonathon Masters, "Confronting the Cyber Threat," Council on Foreign Relations, May 23, 2011, accessed Jun 10, 2013, www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577.*
[17] *Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Cyberpower and National Security, ed Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (USA: NDU Press & Potomac, 2009), 38.*
[18] *Danny Steed, "Cyber Power and Strategy: So What?" Infinity Journal No. 2 (Spring 2011), 22.*
[19] *Yossi Melman, "Outgoing Mossad Chief: Iran won't have Nuclear Capability before 2015," Haaretz, 7 January 2011.*

in this instance enabled the accomplishment of limited objectives and created the conditions for other instruments of policy to be harnessed; a central tenet governing the use of military force too.

Given the regime's obsession with pursuing a nuclear programme, it can be argued that the use of military power is unlikely to have compelled Iran to bow to international will and give up its nuclear ambition altogether. Absent the physical destruction and corporeal harm that military power would otherwise have inflicted, cyber power afforded Israel and the United States the option of implementing an offensive strategy whose non-kinetic character neither provoked a military retaliation from Iran nor drew the international condemnation that a costly and messy military strike would have.[20] Tipping the balance in favour of a cyber attack against Iran's nuclear facility vis-à-vis a military attack was also the doubt whether a conventional air strike would have been unsuccessful in inflicting the desired damage to Iran's nuclear facilities owing to their well dispersed underground locations in mountainous terrain.[21]

The idea of achieving political objectives employing a non-kinetic weapon that conferred the added advantage of deniability was so appealing that President Obama readily acquiesced to the strike. Equally appealing was the downstream effect of a surgical strike on Iran's most heavily guarded nuclear facility- a debilitating impact on morale, and a heightened sense of fear in Iran that its other nuclear facilities too could be similarly targeted.[22] 'Stuxnet' therefore, proved to be a watershed as it illustrated how rather than employ military power, which is often unpalatable to the craven instincts of the electorate and politicians in government, a cyber attack presents the game changing option of achieving limited objectives with precisely directed force in cyberspace.[23] Statecraft had at last discovered the ideal tool; one that not just avoids the friction generated by a military strike but also allows the implementation of strategy that deferentially acknowledges the continuing relevance of Clausewitz's counsel that it is friction generated by war's effect on domestic politics that determines the outcome of strategy.

[20] *Barzashka, "Are Cyber-Weapons Effective," 49.*
[21] *David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown, 2012), 243-247.*
[22] *Lukas Milevski, "'Stuxnet' and Strategy," JFQ, Issue 63 (4th Quarter, 2011): 65.*
[23] *Sanger, Confront and Conceal, 236 (Illustration).*

The Nature of the Beast

From its fledgling roots in Alvin and Heidi Toffler's 'Third Wave', cyber warfare has matured into a strategic alternative to kinetic warfare. The cyber attacks on Estonia and Georgia did foreshadow the inception of a new form of warfare at the strategic level but stopped short of helping policy planners gauge the full potential of this instrument of power since it was either employed in conjunction with conventional military power (Georgia) or exploited in pursuit of limited objectives (Estonia).[24] Therefore, using Georgia as an exemplar to infer that cyber attacks, albeit capable of denying the enemy use of his information systems, are incapable of coercing him to do our will without the help of force being brought to bear on him in the other domains of warfare, is anachronistic.[25] So too is the contention that cyber attacks are, at best, capable of accomplishing objectives only at the operational and tactical levels. Georgia was five years ago; the computing power of IT systems and the disruptive technologies that derive from it are three generations ahead of what they were in 2009.

The expanding portfolio of cyber attacks as a consequence of the rapid advancement of technology presents governments with a wide range of policy options. By virtue of their clandestine employability, whether in war or peace, and the ability to strike at the enemy's vulnerability to accomplish politico-military outcomes that confer strategic advantage, cyber attacks are increasingly being viewed as a special operation in the digital domain.[26] To say, therefore, that they confer strategic benefit only when complemented by conventional warfare is acknowledgment of not having the political and strategic dexterity to modify the objectives to harness the awesome potential of this unique tool in the manner that 'Olympic Games' did. The unrestrained manner in which cyber attacks (which include cyber espionage) are being exploited even during peace to realise interests and inflict harm on adversaries has justifiably led analysts to conclude that they are indeed capable of influencing relations between nations. The fact that America and China elevated concerns over cyber intrusions to the top of the agenda of the 2013 summit meeting between the heads of the two countries substantiates this conclusion.

---

[24]Stephen Blank, 'Web War I: Is Europe's First Information War a New Kind of War?', ComparativeStrategy, Vol. 27, No. 3 (May 2008): 227–231.

[25]Stephen W. Korns and Joshua E. Kastenburg, "Information Warfare and Deterrence," Parameters, Vol. 38, No. 4 (Winter 2008/2009): 60.

[26]Milevski, "'Stuxnet' and Strategy," 65.

A common charge against cyber attacks is that all the apprehensions about their destructive potential lie in the domain of rhetoric, and the world has been witness to little by way of evidence to substantiate the fears that a digital death is indeed a reality. What has been overlooked is the nature of the beast. One of the principal reasons for cyber attacks of the magnitude of 'Stuxnet' or 'Shamoon' (a cyber attack on Saudi Aramco discussed later in the article) being few and far between is the self-depleting nature of this tool, which necessitates judicious and sparing use for strategic purposes. The frequency and complexity of cyber attacks that can be delivered are predicated on the number and type of system vulnerabilities the attacker identifies. The portfolio of exploitable vulnerabilities depletes rapidly as security firms are quick to release security patches as and when the vulnerabilities are revealed. A zero-day vulnerability is, therefore, no longer an exploitable vulnerability once it has been exploited. More importantly, given the immense advantage that accrues from being discreet about one's strong offensive cyber capability so as to retain the flexibility of subsequently exploiting it to achieve strategic goals without fear of attribution, it is more likely that countries would refrain from declaring the coercive cyber attack capability they possess, much unlike the case with military capability.[27] Countries are even willing to risk the safety of their domestic IT systems by building an arsenal of cyber attack and espionage tools for use against adversaries, but not revealing the vulnerabilities these tools prey on even to their own agencies whose systems suffer from the same vulnerabilities. This trade-off favouring offense over defence also reflects the shocking truth that the more substantial a country's investment in offensive tools, the greater is the incentive to keep its capability a secret so that security vulnerabilities in widely used software remain unfixed and available for exploitation when required.[28]

Another aspect worthy of note is that it is not uncommon for countries to refrain from declaring that they have been subjected to a cyber attack for fear of: embarrassment; loss of credibility of their cyber defence capability; boosting the morale of the adversary; and, possibly because they too freely employ cyber attacks against their adversaries. Iran might indeed have refrained from officially protesting against 'Stuxnet' because of either or all of these reasons.[29] It is the

[27] *Thomas Schelling, Arms and Influence, (London: Yale University Press, 1966), 36.*
[28] *Joseph, Menn, "Special Report: US Cyberwar Strategy Stokes Fear of Blowback," Reuters, May 10, 2013, accessed Jun 10, 2013, www.reuters.com/article/2013.*
[29] *Gary D. Brown, "Why Iran Did'nt Admit 'Stuxnet' Was an Attack," Joint Forces Quarterly, Issue 63, 4th Qtr (2011): 71-73.*

collective impact of these attributes that impedes comprehensive realisation of the destructive potential of this tool.

Cyber Power as an Instrument of State Policy

Here again, what stands in the way of cyber power being acknowledged as an instrument of statecraft capable of independently accomplishing policy objectives is the unfortunate truth that there is little understanding of the potential of this tool outside of the technical community. Its novelty and technology-intensive character make it an esoteric subject that strategists and politicians alike prefer to maintain a discrete distance from.[30] What is not taken cognisance of is the dangerous reality that norms, ethics and deterrence have little meaning in this domain where attribution is difficult, deniability is easy and there is no legal framework to determine the legitimacy of actions.[31] Absent a political framework to regulate their use, cyber attacks are being unleashed with impunity to achieve political, economic and military objectives, albeit limited in scope.

The Intellectual Debate

The contentious debate in the context of cyber war also stems from the insistence of critics that it cannot be treated at par with war in the other domains as it does not meet the Clausewitzian conditions of traditional war, i.e. although its effects can be warlike, it is not war in the absolute sense since there is a conspicuous absence of violence that causes death and physical destruction in the manner that conventional war does.[32] As a consequence, they aver, it cannot coerce the enemy to do our will. Implied by this is the contention that cyber war cannot be instrumental in achieving the political purpose of war since it is incapable of rendering the enemy hors de combat and leaving him with no option but to succumb to the attacker's will.

It is these contentions that the article seeks to dismiss. When the concepts associated with war itself are nebulous and contested, it may not be correct to deterministically conclude that cyber war is not war in the true sense.[33] Quite

[30]*Colin S. Gray, "Making Strategic Sense of Cyber Power: Why the Sky is not Falling," Strategic Studies Institute, US Army War College (April 2013): 6, accessed Jul 2, 2013, www.StrategicStudiesInstitute.army.mil*
[31]*Paul Cornish et al, On Cyber Warfare, Chatham House (Great Britain: Latimer, 2010): 32.*
[32]*Peter Paret, 'Clausewitz', in Makers of Modern Strategy from Machiavelli to the Nuclear Age (Princeton, NJ: Princeton University Press, 1986), 199.*
[33]*Betz, "Cyberpower in Strategic Affairs," 691.*

contrary to the charge that it lacks the ruinous potential of military force, full-fledged cyber attacks can indeed cause large-scale power disruptions, communication failures, transportation breakdowns, traffic snarls and other downstream effects that are bound to eventually cause death and destruction. The attacks may not visibly deliver the kinetic force that military power does to inflict immediate and widespread damage on the enemy but what is indisputable is that they too can trigger large-scale devastation, albeit in an indirect, sequential and delayed manner. The destruction of the centrifuges at the Natanz plant by 'Stuxnet' was illustrative of this second-order downstream effect of a cyber attack although there were no deaths. Yet another argument favouring the treatment of cyber attacks as acts of war is the strong possibility of such second-order damage provoking a military response from the victim thus precipitating violence.[34] NATO's Strategic Concept, which through a modification of its charter now treats cyber attacks as a threat to Euro-Atlantic security and permits the invoking of Article 5 in the event of a future cyber attack against any of the alliance members, validates this argument.[35]

Much in contrast with conventional war, which is viewed as a continuation of policy by other means, cyber war virtually renders political intercourse insignificant by arming nations with the digital means to influence or coerce adversaries even in peace.[36] Using cyber attacks as a policy instrument to achieve the political aim conforms to Clausewitz's counsel that 'if the political goals are limited, then the policy instrument should seek to coerce rather than decimate the enemy. In the prevailing environment where international and domestic audiences seldom countenance resort to purposive violence to accomplish objectives, it is only appropriate that the policy instruments employed are commensurate with the political objectives desired, and do not inflict needless death and destruction. After all, isn't Clausewitz criticised for his obsession with force. 'Stuxnet' epitomised this strategic restraint; it was instructive in the precise choice of policy instrument to accomplish political objectives without precipitating violence.[37] Conscious of the adverse consequences of using military power against Iran, the architect(s) of 'Stuxnet' were astute in modifying both

[34]*Mathew C Waxman, "Cyber-Attacks and the Use of Force," The Yale Journal of International Law, Vol. 36 (2011): 425-430.*
[35]*Haly Laasme: "Estonia: Cyber Window into the Future of NATO," Joint Forces Quarterly, Issue 63(4th Quarter 2011): 60.*
[36]*Cornish et al, On Cyber Warfare, 32.*
[37]*Colin Gray, Another Bloody Century (London: Weidenfield and Nicolson, 2005), 24.*

policy objective and strategy to that attainable by the means- cyber power. While it is true that recourse to a cyber attack may, at times, warrant a less ambitious initial political objective, the scale-down would still be preferable to violence and its adverse ramifications. Unlike conventional war, which inflames emotions, and runs the risk of becoming an end in itself because of the tendency of violence to fall prey to escalatory dynamics and become self-feeding, a cyber attack, owing to its unique non-kinetic and clandestine nature, poses relatively less risk of engendering violence on a similar scale. Policy is thus able to exercise control over the 'ways' employed without ever being in danger of getting subordinated to the strategy that it created; an enduring precept of war, which excessively militarised strategies have been guilty of violating in the past.

In support of Clausewitz's dictum that the nature of war is immutable while its character is not, 'Stuxnet' exemplified the manner in which technology has essentially transformed the character of war.[38] Cyber attacks may not replicate the violent character of traditional war but what must not be ignored is that the character of war is always determined by the relative combat power of the adversaries, which in large measure dictates the ways and means of conflict employed, as also how adversaries choose to fight. A nation may choose to avoid attrition by avoiding force on force confrontation with its adversary's superior conventional military and opt instead for the more conservative asymmetric strategy of harnessing cyber power to attack the enemy's critical infrastructure for accomplishing political goals.

Cyber attacks that are politically motivated and employed with the intention of coercing the adversary may well be equated with an offensive strategy that employs sea power, air power or land power.[39] Territorial conquest and the destruction of militaries need not be the only tangible ways to coerce the enemy; cyber attacks that can inflict damage of an unfathomable degree can be as persuasive as a military course of action in browbeating the enemy to submission. Cyber power confers the ability to strike at the heart of the enemy without having to contend with its air, sea and land power. The operational philosophy of 'shock and awe' attributed to the effective use of air power and precision guided munitions could well be replicated in the cyber space domain at far less expense and collateral damage.[40] A full-scale cyber conflict, as the one between Russia and

[38] *Colin Gray, Modern Strategy (Oxford: Oxford University Press, 1999), 101.*
[39] *John Arquilla, "Cyber war is Already Upon Us," Foreign Policy (March April 2012): 84-85.*
[40] *Martin Shaw, The New Western Way of War (Cambridge, UK: Polity Press, 2005), 25-35.*

Georgia, even bore resemblance to the grammar of war that Clausewitz wrote about, albeit in the form of attacks and counter-attacks in the cyberspace rather than the sequenced battles and tactics on the battlefield.[41]

Conditional upon their severity and extent, cyber attacks too can be as instrumental in rendering the enemy defenceless as destroying combat power using military means. The well-orchestrated cyber attack on Saudi Aramco in September 2012, believed to be politically motivated and perpetrated by Iran, showcased the potential of this vector to cripple a country's vital industry. Providentially, while the attack did not succeed in its purpose of disrupting the company's oil production or export functions, the devastating impact on world oil prices and the financial markets had that happened can well be imagined given that Aramco accounts for more than 10% of world oil production.[42] Without causing physical damage of equipment or loss of life, the attack imposed substantial monetary loss and time penalty on the Saudi government, not to mention the inconvenience. A physical sabotage may have been easier to rectify; not so 30,000 computers, which could not even be booted to life after the attack. Should such an attack occur on a much larger scale encompassing a country's financial, military and government networks, the consequences would be devastating. Faced with the crippling loss of critical networks, as also the inability to function effectively, the victim would have little option but to give in to the attacker's will.[43]

It is not just during hostilities that cyber attacks can do grave harm; the ability to furtively gnaw at a potential adversary even during peace makes it a highly versatile policy instrument. Particularly harmful is the erosion of a country's technological superiority from the cyber theft of intellectual property and sensitive technologies belonging to defence contractors and research institutions. Losing a few documents or scraps of important information is one thing; losing data and intellectual property in excess of the information contained in the Library of Congress is another altogether.[44] Some of the biggest enterprises like NASA and Lockheed Martin have reported the theft of vital information related to strategic projects; significant of which, was the loss of several thousand

[41] *Gray, Modern Strategy, 93.*
[42] *Reuters, "Aramco says Cyberattack was aimed at Production," New York Times, Dec 9, 2012, www.nytimes.com*
[43] *Thomas Rid, Cyber War Will Not Take Place (England: Hurst, 2013), 55-65.*
[44] *US DoD, "Strategy for Operating in Cyberspace (July 2010)," 10.*

gigabytes of information related to the design of the F35 combat aircraft and its revolutionary electronic warfare suite.[45]

In 2011, more than 70 companies and governments were victims of cyber thefts that deprived them of several million dollars of proprietary information. Symantec Corporation's estimate is that in 2012 the average per capita cost of data breach was $194 to the United States; $191 to the Danish government; and, $124 to the United Kingdom.[46] Over a period of time these losses will serve to blight innovation and eventually blunt the economic, technological and military superiority of highly developed knowledge-based societies.[47] China served a foreboding reminder of just such a possibility when in 2012, Sinovel, a Chinese manufacturer of wind turbines used nefarious means to steal software related to wind turbines, from its American supplier, AMSC. The implication of this cyber theft was a dramatic fall in the latter's revenue (90%) shortly thereafter,[48] which forced AMSC to cut its workforce by 30% at a time when the US labour market was already suffering record unemployment.[49] When viewed from the perspective that China recently overtook the United States as the world leader in wind energy capacity, the incident says a lot about the instrumentality of cyber espionage.[50] So does the disastrous closure of the Canadian telecommunications firm Nortel as a consequence of losing intellectual property to cyber espionage reportedly perpetrated by the Chinese firm Huawei.[51]

Since war is a continuation of political intercourse by other means, the underlying political objective of a full-fledged cyber attack would be amply evident from the temporal coincidence between its manifestation and an ongoing source of friction. The political purpose of the cyber attack on Estonia in 2007, though not openly stated, was evident: to dissuade it from relocating a monument of great significance to Russian sentiment. The credibility of the attacker's resolve and intent to compel the enemy are reflected in the destructiveness of the cyber attacks. Rather than harness the unique advantages of stealth and deniability that

[45] *Clarke and Knake, Cyber War, 232-235.*
[46] *Symantec Corporation, Internet Security Threat Report 2013, 19.*
[47] *Adam Segal, "Chinese Computer Games," Foreign Affairs, Vol. 91, Issue 2 (Mar/Apr 2012): 15.*
[48] *Erin Ailworth and Eugen Freund, "Engineer Guilty in Software Theft," The Boston Globe, 24 September 2011.*
[49] *Peter Behr, "Chinese Company Accused of Economic Espionage in Wind Tunnel Case," Environment and Energy Publishing, 26 Jan 2012.*
[50] *Ashvin Ahuja et al, "An End to China's Imbalances," International Monetary Fund, WP/12/100 (April 2012):7*
[51] *Nigel Inkster, "Chinese Intelligence in Cyber Age," Survival (Feb-March 2013): 61.*

cyber power confers, it would be self-defeating to hamstring oneself with the hackneyed logic that the political intent behind its employment must be declared. That Estonia did reverse its original decision of moving the statue is testament to the political success of this strategy.

Conclusion

Clearly, therefore, it is the inability of scholars to break away from the logic of Clausewitz's insistence on the centrality of combat to strategy that has prevented the acknowledgement of the true potential of cyber attacks and the threat they pose to national security. Policy planners will only be guilty of jeopardising the critical infrastructure of their nations if they fail to realise the unique ability of cyber attacks to translate force into violence; as Colin Gray asserts, electrons are no less dangerous than any other weapon that delivers kinetic force. Strategic thought ought not to discount the potential of cyber attacks to do grave harm just because cyberspace is a domain that lacks physicality and cyber power tends to be intangible in its effects.[52]

While it is conceded that strategy and capability development ought to be predicated on interests and not fixated on threats, it would be unwise to ignore the importance of cyber attacks in the threat spectrum. It was only when 9/11 happened that the United States championed the global war on terror, which till then was a crime rather than war against the international community; hopefully we will not have to wait for a cyber 9/11 to galvanise us into acting in a coordinated fashion against this malevolent vector.

Implicit in the claim that kinetic force is not the only instrument by which strategic objectives can be achieved in cyberspace is the logic that physical damage and corporeal harm need not be the metric of success or victory. The perpetrators need no longer be equipped with hi-tech military weapons to destroy the enemy. The actions of a rival state can be influenced, and political and strategic goals achieved in limited measure, without bombing them into submission.

[52]*Colin S. Gray, "Making Strategic Sense of Cyber Power: Why the Sky is not Falling," Strategic Studies Institute, US Army War College (April 2013): 16, accessed Jul 2, 2013, www.StrategicStudiesInstitute.army.mil*

Sabotage, subversion, espionage, financial chaos, industrial disruption and many other depredations can be inflicted on the adversary using surreptitious cyberspace techniques, which were once the preserve of vandals and ethical hobbyists but have now morphed into tools of warfare.[53]

❀ ❀ ❀

About the Author

Commissioned into the Indian Navy in Jan 1986, Cmde KG Vishwanathan, VSM, is a graduate of the Defence Services Staff College, Wellington, Naval War College and the Royal College of Defence Studies, UK. In addition to a Master's Degree in Science and MPhil from Mumbai University, he has a Master's Degree in International Security and Strategy from King's College, London, where he was the recipient of the Richard Edis Award 2013. He is presently the Deputy Commandant of the Naval War College, Goa. The author can be reached at vish_gan@yahoo.com

[53]*Ram Mohan, "The Veterans of the Future Will Be Those in Computer-Based Combat," accessed 25 December2013, http://www.securityweek.com.*