Cyber aspects of non kinetic warfare

Post World War-II, there has been a paradigm shift in the nature of conflict and pattern of statecraft primarily due to; advent of nuclear weapons, Revolution in Military Affairs, rapid advancement in information technologies, rise of Non State Actors and effects of globalization. These transformations have made use of military or kinetic options for advancing states' policies less attractive, as not only the war is too costly, it is also too damaging – even to the victor. Consequently, the non-kinetic dimensions of statecraft i. e. Informational, Diplomatic and Economic have gained ascendancy and prominence in shaping the global security narratives. Historically, the Cold War model is the most sustained and successful application of non-kinetic domains where dissolution of USSR was brought about through application of non-kinetic means.

Since our independence, Pakistan has remained in a state of perpetual conflict with its arch rival India. Until 28 May 1998, the main threats to Pakistan were primarily in the kinetic domain and so were our responses. However, after the overt nuclearization of South Asia, the threat paradigm has been further compounded to involve host of kinetic as well as non-kinetic challenges not only from India but also from other hostile or potentially hostile actors. In our case, there are many drivers for this shift, but nuclear capability and the ongoing conflict in Afghanistan remain the most important ones. A strategic reappraisal of our security calculus particularly within the non-kinetic domain is extremely important.

Aforesaid, carry out an in-depth study of Non Kinetic Warfare and its application in today`s environment and the challenges it poses to Pakistan with a view to recommending suitable response options to prepare armed forces to effectively meet challenges it poses to Pakistan with a view to recommending suitable response options to prepare armed forces to effectively meet challenges at hand.

SUB THEME

During last two decades, role of information technology has enhanced considerably in warfare. Today, through the application of latest cyber technology, massive quantities of information concerning individuals or organizations can be collected, processed, stored and targeted. Attacks in the domain of cyber warfare can disable official websites and networks, disrupt or disable essential grids – among many other possibilities. With the rapid spread of information technology in Pakistan, vulnerability to such attacks has also increased manifold.

Aforesaid, carry out an in-depth study of cyber Warfare as an element of Non Kinetic Warfare, its application in today`s environment and the challenges it poses to Pakistan with a view to recommend suitable response options at national and army level.

ABSTRACT OF RESEARCH ON CYBER ASPECTS OF NON KINETIC WARFARE

The non kinetic warfare is a new buzzword these days. To lay the conceptual foundations of non-kinetic warfare, it is pertinent to understand the terms kinetic and non-kinetic. We can differentiate between “ kinetic” and “ non-kinetic” actions basing on whether it has a physical damage i. e. injuring, killing or destruction of an intended enemy. In the modern context, non kinetic warfare is a synonym to unconventional or non-traditional methodologies. To be effective, non kinetic warfare may precede or succeed kinetic application. This study briefly dilates upon the concept of non kinetic warfare, its materialization in different forms with main focus on cyber aspects of non kinetic warfare.

To this end, an attempt has been made to study the whole range of cyber warfare, assess threat to Pakistan and suggest suitable measures to exploit the true potential of this new phenomenon, simultaneously defending own vulnerabilities. Laying down short and long term measures, establishment of a policy making organization at national level and a cyber warfare cell at armed forces level has been recommended. The starting point of the whole structure however, would be the improvement of awareness about information technology among masses.

PREFACE

When history is at its turning point, nations have three choices. First is to live in the past; relishing triumph, elaborating myths, and eventually becoming a part of the past. The second choice is to fight change. Certainly, all change is not for the better. The third alternative is to embrace the future with all of its uncertainties and becoming part of the change.

Uncertainty has always been essential part of war. With a large variety of war waging means available, the enemy will be much more dynamic, versatile and unpredictable in nature. True face of the enemy might never reveal whereas the damage is caused beyond proportions.

Contemplation of such scenarios has led the world to the conceptualization of rather a new dimension called non kinetic warfare. Within the sphere of non kinetic warfare, though, threats emanating from use of cyber space assume greater importance and are hence the focal point of this research study. In this paper, I have dilated upon the subject of cyber warfare as an emerging arena for waging non kinetic wars. In the end, I have examined cyber threat in the context of Indo-Pak Sub-continent and put forth some useful recommendations to prepare ourselves for the future.

CHAPTER – I

CYBER DIMENSION OF NON-KINETIC WARFARE

" To win one hundred victories in one hundred battles is not the acme of skill.

To subdue the enemy without fighting is the acme of skil[1]l."

Sun Tzu

Introduction

Post Cold War developments have brought about two paradigm changes in the international relations; first, splitting up of states` power between State and Non State Actors (NSAs) and second, surfacing of geo-economics as the essential ingredient of interstate relationships. The active role of supranational organizations e. g. United Nations and other regional / economic forums, proliferation of nuclear weapons, Revolution in Military Affairs and advancements in information technology have rendered the use of military or kinetic options less attractive for the developing states, not only because of the cost/consequences of all such conflicts, but also the inherent difficulty to keep them limited. It is potentially damaging too – even to the victor. As a result, the non-kinetic dimensions of statecraft i. e.

Informational, Economic, and Diplomatic, have gained significance in moulding the global security narratives.

Conflict and war are inherently kinetic in execution. As Carl von Clausewitz said, true competitors would rarely engage in conflict, as mutual destruction would surely occur. The technological advantage afforded by faster communications, precision guided munitions and improved surveillance and reconnaissance means is difficult to ignore. Computer network based warfare is rising in utilization. Several models and analogies have been argued to explain deterrence and conflict in cyberspace.

Cyber warfare involves non physical attacks on information data and its collection process aimed at damaging, disrupting or destroying decision making process. It is both offensive and defensive, ranging from methods that prohibit the enemy from exploiting information to corresponding measures to guarantee the availability, reliability, , and interoperability of friendly information assets.

While eventually military in nature, cyber warfare is also waged in political, economic, and psycho-social arenas and is applicable over the entire national security spectrum from peace to war and from ‘ tooth to tail.’ It capitalizes on the growing sophistication, connectivity, and reliance on information technology (IT). That is why, as we address the challenges of the 21st century, we must take into account rapid technological developments in information management and dispensation, that are indicative of, many believe to be the beginning of a post-industrial age; the Information Age.

Pakistan's Armed forces, like others, are becoming increasingly dependent upon the civilian information infrastructure, which is essentially world-wide. Commercial systems are no less vulnerable than their military counterparts. In this situation, it is critical for Pakistan to work out a strategy to utilize the benefits of the information technology, while revitalizing itself against the threats posed by Cyber warfare.

Pakistan is in the evolution process of developing a meaningful approach to develop and employ Cyber warfare means against the enemy and defend against such attacks. The sphere of Cyber warfare falling in the strategic domain requires response at the national level in general and at army level in particular. Therefore, there is a need to develop an understanding of the cyber warfare, analyze the threat to Pakistan, and recommend measures to enhance national war effort.

Aim

To carry out an in-depth study and analysis of cyber aspects of Non Kinetic Warfare, highlighting threat dimensions, response options and directions for the future with particular reference to Pakistan.

Scope

An Endeavour will be made to seek answer to the following questions:-

a. What is the genesis of Non Kinetic Warfare?

b. How does Non Kinetic Warfare manifests in various forms?

c. The conceptual contours of cyber warfare?

d. The prospects of cyber threat in our scenario?

e. How to prepare ourselves for the future?

CHAPTER – II

CONCEPTUAL CONTOURS OF NON KINETIC APPLICATIONS

General

6. The nuclear overhang and the rising cost of warfare both in men and material, envisage that the future wars will predominantly be fought in the non-kinetic domain. These wars will incorporate the will of the people as primary target. The growing significance of non-kinetic approaches and methods in present strategic environment necessitate the development of credible non-kinetic capabilities by the contemporary states, in addition to the kinetic deterrence, to project power; solve problems and secure interests.

7. It is about time to reject the conventional concept of war fighting in the kinetic realm and think about solving conflicts in ways other than those of causing destruction and bloodshed. In this chapter an effort will be made to examine the rapid growth in the arsenal of non-kinetic warfare, so as to highlight appropriate actions that states and their predominantly kinetic armies could undertake in the future. The terms ‘ kinetic’ and ‘ non-kinetic’

are new buzzwords in the military literature at present, although, Sun Tzu had already described the non-kinetic approach as “ the pinnacle of the art of war”[2], during the 6th century BC.

The Conceptual Foundation and Definition

7. To lay the conceptual foundations of “ non-kinetic warfare” it is pertinent to understand the terms “ kinetic” and “ non-kinetic”. Very few “ United States Department of Defense (DoD)” resources define the term “ kinetic”. This word is absent from the “ DoD Dictionary of Military and Associated Terms”[3]and not clearly defined in other major doctrinal publications of the United States Joint Staff, the Army, Navy or Marine Corps. “ The Air Force Doctrine Document 2 (AFDD2) – Operations and Organization” is perhaps the only major United States’ doctrinal publication that attempts to define the terms “ kinetic” or “ non-kinetic”. Under the heading “ Effects-Based Considerations for Planning”, the document states that:-

“ Kinetic actions are those taken through physical, material means like bombs, bullets, rockets, and other munitions. Non-kinetic actions are logical, electromagnetic, or behavioral, such as a computer network attack on an enemy system or a psychological operation aimed at enemy troops. While non-kinetic actions have a physical component, the effects they impose are mainly indirect- functional, systemic, psychological, or behavioral”[4].

8. The above quoted document uses means to characterize kinetic actions, however non-kinetic actions are describe with the help of effects. This is an incongruent way of defining a pair of antonyms. It may not satisfy all the situations. For example: firing a warning shot into the air can be classified

both as kinetic and non-kinetic? It fits into both of the Air Force Doctrine Document (AFDD) – 2 definitions- i. e. use of physical means (kinetic) as well as indirect effects it causes (non-kinetic). It is, therefore, imperative to define both terms in a uniform manner, either depending upon " use of means" or " the ensuing effects". While the similar means may be employed for both " kinetic" and " non-kinetic" actions, the method / technique of their employment will decide its kinetic or non kinetic application. More often than not, a single action can have both tangible and intangible effects. We can differentiate between " kinetic" and " non-kinetic" actions basing on whether it has a physical damage i. e. injuring, killing or destruction of an intended enemy. In simple words, " kinetic" results into inflicting physical damage on the anticipated target; while " non-kinetic" is the effect of that damage. For example, even though North Korea's nuclear test in early February 2013, involved physical destruction, its intended effects were a show of strength and deterrence to the enemies. Hence, this test fire may be termed as a non-kinetic action.

Historical Perspective

11. The concept of non-kinetic approach towards warfare is as old as warfare itself. Many of history's greatest generals had a natural sense for it. Like the Sun Tzu began his discourse on warfare in his famous book " Art of War" by saying:

" Generally, in war the best policy is to take a state intact; to ruin it, is inferior to this. To capture the enemy's army is better, than to destroy it; to take intact, a battalion, a company or a five-man squad is better than to kill them. For, to win one hundred victories in one hundred battles; is not the acme of skill, to subdue the enemy without fighting is the acme of skill……… Thus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting and overthrow his state without prolonged operations. Your aim must be, to take All-under-Heaven intact. So your troops are not worn out and your gains will be complete. This is the art of offensive strategy[5]".

12. While Sun Tzu's immense work on the art of war is primarily about the way of fighting, it is evident from the above mentioned quotation that, he did not idealize kinetic operations as the perfect route to victory. He preferred to win through ideas without resorting to fighting and destruction. Thus, according to him, non-kinetic strategy was superior to one that was kinetic.

13. In 1989, William S. Lind proposed that " the emerging Fourth Generation Warfare would be dispersed, undefined due to nonexistent distinction between war and peace"[6]. In this kind of warfare the objective has transformed into " non-kinetic impairment of the enemy`s will" instead of " the kinetic destruction of military forces", This is because of the prevalent sociopolitical-economic environment that the kinetic warfare, today, is more of a liability than at any time in history.

14. In the middle of the 20th century, the British strategic theorist B. H. Liddell Hart advocates " the indirect approach" in strategy. The wisest strategy, he argued, avoids the enemy's strength and probes for weakness.

Various Dimensions of Non-kinetic Warfare

15. Prevalent Environment. At present, the anarchic state structure almost globally leads to a state of continued conflict. These conflicts are mostly in

the psychological domain. In addition, the advancements in the informational, diplomatic, economic, ideological, and technological means have relegated the military prong to merely a support role. With expansion in the IT and growing globalization, " it has become possible now to generate desired effects through non-lethal components of DIME[7](Diplomatic, Informational, Military & Economics) matrix."

16. Strategic Prospects. Geo-economic environment has intensified interstate competition, reducing space for kinetic conflicts; thereby moving them into the ideological, informational and cyber domains. Resource wars are the new phenomena, coming up in the face of quickly depleting resources and rapidly growing population. Super-national organizations or aligned states have greater share in defining economies and policies worldwide; hence non relevance with their agenda is a convincing threat scenario. Hence, Nations are being exploited by adversarial states, non-state actors, International Financial Institutions, international media, publishing houses, think tanks, intellectual and writing forums, human right organizations, children and labor laws, and international trade agreements like, World Trade Organization and International Atomic Energy Agency etcetera.

17. Non-Kinetic apparatus. The commonly used apparatus is:-

a. Military (to compliment the non-kinetic domains).

b. Diplomatic tentacles, traders, economists, bankers, politicians, Non State Actors, Trans-national Companies, Multi-national Companies, Non-governmental Organizations & international organisations like United nations, European Union, International Court Justice, World Bank etc.

18. Domains of Non Kinetic Challenges

a. Information & Media Operations. The sole aim of the information and media operations is to flood massive volume of information into the mind of the consumer. This flooding leaves the audience unable to filter the right from wrong. Whether information is believed, ignored or distrusted will depend upon the intellectual standing of the receiver and reputation and credibility of the sender.

b. Cyber Warfare. Attacks in this domain can disable / deny official networks and websites, disrupt or disable vital services, steal or modify classified data and cripple financial systems & electricity grids — among many other possibilities. Most recent applications are[8]:-

Attack on Iranian Natanz nuclear enrichment facility by Stuxnet virus.

Indian and Pakistan hackers defacing and hacking each other’s websites.

There is even talk of US predator drones’ command & control systems becoming a victim of cyber warfare.

Russia and China employ armies of cyber experts for hacking while raising of a US Cyber Command and declaration by US to consider a cyber attack as an act of war speaks of its current and future importance.

c. Diplomacy. In 21st Century, diplomacy has eclipsed military as the most important tool of statecraft as now it alone can impair the will of an adversary to a level of shaking down willingness without having to resort to kinetic actions.

d. Soft Power. It is the ability to use others through co-option and luring in and its currencies are values, ethics, culture, policies and institutions.

e. 4th Generation Warfare, Sub Conventional Warfare & Proxies. These are kinetic application tools of Smart Power, where while remaining under full blown military / kinetic applications, they work to induce enemy's political decision makers that their strategic goals are either unattainable or too expensive for the perceived benefit.

f. Non-kinetic energy weapons. To enhance the efficacy of Non kinetic Applications certain explicit theories have been devised which aim to draw benefits out of chaos and disorganization. Visible expressions are evident in present times. Salient ones are:-

Creative Chaos Theory[9]. Here existing chaos is either aggravated or deliberately created to force major adjustments / modifications in state structures. Libya & Arab Spring are recent examples; Pakistan needs to draw lessons from these situations as similar applications are within the realm of possibility.

Shock Doctrine/ Disaster Capitalism[10]. This theory asserts that states deliberately profit from public perplexity following man-orchestrated or natural disasters. Contracting out of oilfields in Iraq to western oil companies is a clear expression.

Disruptive Technologies[11]. New technology has also enabled states to cause extensive damages within the natural and human spheres to their adversaries. Diagram – 1haarp_wave_propagation. jpg

HAARP Theory. It proposes tampering of ionosphere & geo-physical domain for purposeful military and civilian application[12]. Visible signs of its manifestation exist in terms of weather and geo-physical manipulations[13].

Mind Control Sciences[14]. The theory revolves around making a deliberate attempt to manage public's perception on a subject through sensitization. Although in its early stages of development, it is a potent threat for the future[15].

Extremely Low Frequency & Directed Energy Weapons[16]. (Diagram – 1) ELF uses radio waves as a weapon to create incapacitation and disruption without resorting to destruction; whereas Directed Energy weapons are the newest in the range of destructive weapons but with tremendous potential and range of utility. Applications in this domain are presently experimental in nature but fast reaching operational status.

18. Conclusions. Following important conclusions emerge which help assimilate non-kinetic challenges and thus merit attention:-

Non-kinetic means will be preferred over the kinetic means to achieve national aims and objectives.

The main purpose of non-kinetic application will be to trigger, exploit, or amplify internal instabilities and fault lines of the target nations in order to impair national will and resolve.

Information technology and electronic & print media will be the primary means of application.

Cyber domain will be used to augment these means, so as to magnify future threats. Ever improving technology will add to its effectiveness.

Kinetic domain will remain relevant as means of deterrence, while non-kinetic means are concurrently strengthened and developed.

CHAPTER – III

CYBER WARFARE – AN EMERGING NON KINETIC DIMENSION

It has belatedly begun to dawn on people that industrial civilization is coming to an end. It’s unraveling . . . brings with it the threat of more, not fewer, wars-wars of a new type[17].

Alvin and Heidi Toffler

General

23. Cyber warfare is an outcome of information age paraphernalia like satellites, electronic mailing system, internet, computers and micro-chip. Growing use of these tools in all fields of life, makes it mandatory for various elements of national power to absorb, store, evaluate, use and exchange large volumes of information. This necessitates establishment of versatile management structures. These systems invariably contain inbuilt strengths and vulnerabilities. Exploiting such vulnerabilities of the enemy has come up as a new dimension of war craft termed as cyber warfare.

24. Cyber warfare can manipulate all three components of the nation-state: the people, the government, and the military. This is a new pattern of warfare in which there is no need to send formations of soldiers or armada of

warships, instead computer viruses and logic bombs in microprocessor control units and memory chips, may cause a wide spread disorder of every tier of society including military systems.

Cyber Warfare – Definition, Tools and Techniques

25. Definition

a. Before we can define cyber warfare, it is important to understand Information Warfare (IW) which, in the technical sense has been defined as ‘ Actions taken to achieve information superiority by affecting adversary’s information, information based processes, and information systems, while defending one’s own information, information based processes and information systems’.[18]This being universal in nature does not demarcate the military aspects of IW. Military related definition on IW, as used by U. S. Department of Defence is, ‘ Actions taken to achieve information superiority in support of national military strategy by affecting adversary’s information and information systems while leveraging and defending our information and information systems’.[19]

b. Cyber warfare is defined as “ Non-kinetic, offensive actions taken to achieve information superiority by affecting enemy information based processes, information systems and computer-based networks”.[20]From the definition, cyber warfare appears to be the sub-set of IW that involves actions taken within the cyber space as opposed to the physical space or world. The cyber space is a virtual reality enclosed within a collection of computers and networks. One most relevant to cyber warfare is the internet and related networks (military or civil) that share media within or with the internet.

26. Characteristics of Cyber Warfare.[21]Attached as Annex A.

27. Potential Cyber Attack Weapons.[22]Attached as Annex B.

Cyber Dimension of Non Kinetic Warfare

28. The Conceptual Framework

a. Once we talk of cyber dimension of non-kinetic warfare then all the related terms like software war, net war, hackers' war, cyber attacks and cyber terrorism converge at one point becoming synonymous to each other. The tools, modus operandi, actors and even the underlying philosophy; all become part of Non Kinetic warfare. Dominant feature, however, remains the use of cyber space as a medium to wage war and cause massive disruption.

b. Due to inexpensive availability of IT tools, likelihood of cyber attacks as means of non-kinetic warfare has become high. Such attacks can be launched by terrorists to spread terror, by criminals for petty financial gains or by nation-states who cannot afford to wage war against their adversaries through conventional means. These will not only target the web sites of government organizations and private companies, but can also attack more high-value targets such as the networks that control vital economic or power infrastructures.

c. Possible scenarios of cyber attacks in the realm of non-kinetics can be:-

(1) Deny the target nation, its communications and financial resources.

(2) Cause an absolute failure of the telephone and electrical supply systems. The loss of electrical power only can result in chaos and disorder due to a variety of problems.

(3) Use internet (which includes sites from all the major news sources) to spread fake information or simply disable all the news sources on the internet.

(4) Zero out financial accounts of the important government or private offices, institutions or persons.

(5) Misroute trains, crumple the air traffic control system and cause failure of all utilities.

(6) Through hacking, change the composition of steel at a mill to make it susceptible to cracking in extreme hot/cold weather or manipulate components of a food product to add some amounts more than the normal so that it is large enough to become toxic.

(7) Through computer malfunctions, cause detonation or failure of military weapon systems, leaving a country vulnerable to conventional, or worse, Weapons of Mass Destruction attacks.

(8) Cause widespread environmental damage through explosions at computer-controlled chemical factories, undetected leaks in oil pipelines and the bursting of dams.

(9) Fatalities that would result from these attacks include deaths from transportation accidents, exposure to extreme temperatures caused by power failures, drowning from burst dams, riots etcetera.

29. Actors and their Motives. Hundreds of individuals, groups of people or even nations could be considered as potential actors. Anyone with a computer, modem, and telephone can access almost any portion of the information from any location whereas; detecting and tracing such activity can be extremely difficult. The identified actors are:-

a. Hackers. Although most publicized cyber intrusions are credited to lone computer-hacking hobbyists, such hackers pose insignificant threat of widespread or long-duration damage to national-level infrastructures. A bulk of hackers does not, in fact, have a motive to do so. Nevertheless, their large worldwide population poses a relatively high threat of an isolated or brief disruption causing serious damage.

b. Hacktivists.[23]This is a small population of politically motivated hackers, which may include individuals and groups who have intentions against their own or foreign governments. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups, however, appear bent on propaganda rather than damage to critical infrastructures. Pro-Beijing Chinese hackers over the past three years have conducted mass cyber protests in response to events such as the 1999 NATO bombing of Chinese embassy in Belgrade and the more recent EP-3 incident.

c. Industrial Spies and Organized Crime Groups.[