Cyber Wars:
A Paradigm Shift from Means to Ends

Amit SHARMA[a,1]

[a] *Institute for System Studies and Analysis (I.S.S.A),*
Defence Research and Development Organization (D.R.D.O),
Ministry of Defence, India

Abstract. The last couple of decades have seen a colossal change in terms of the influence that computers have on the battle field, to an extent that defence pundits claim it to be a dawn of a new era in warfare. The use of computers and information in defence has manifested into various force multipliers such as Information Operations, C4I2SR Systems, Network Centric Warfare, to the extent that commentators are terming this information age as a Revolution in Military Affairs (RMA). These advances have not only revolutionized the way in which wars are fought, but have also initiated a new battle for the control of a new dimension in the current contemporary world: The Cyber Space.

Over time cyber warfare has assumed the shape of an elephant assessed by a group of blind people, with every one drawing different meanings based upon their perceptions. Under these circumstances there was a gradual paradigm shift in military thinking and strategies, from the strategic aspect to the tactical aspect of cyber warfare laying more emphasis on cyber attacks and counter measures. This resulted in the formation of a notion that cyber warfare or information warfare is a potent force multiplier, which in a sense downgraded the strategic aspects of cyber war to a low grade tactical warfare used primarily for a force enhancement effect. The author believes this is wrong, cyber war is a new form of warfare and, rather than cyber war merely being an enhancement of traditional operations, traditional operations will be force multipliers of cyber war.

This paper tries to shatter myths woven around cyber warfare so as to illuminate the strategic aspects of this relatively misinterpreted notion. This paper will elucidate the scenarios and mechanisms illuminating the process of using the strategies of cyber war, so as to achieve conventional objectives. The paper will also analyze the doctrine and strategies including first and second strike capabilities with regard to cyber war. This paper identifies a paradigm shift from the conventional belief of cyber warfare acting as a force multiplier for conventional warfare to the recognition, that conventional warfare will be acting as a force multiplier around cyber war and hence making cyber war as the primary means of achieving grand strategic objectives in the contemporary world order.

Keywords: Cyber wars; cyber warfare; information warfare; strategy and doctrine.

The opinions expressed or implied in this paper are solely those of the author, and are based on open sources. Under no circumstances these may be correlated or perceived as the views of Government of India in general and the Author's organization in particular.

[1] The Author is Deputy Director/Scientist 'C' in Information Security Division of Strategic Information Dissemination Systems of I.S.S.A., D.R.D.O., Ministry of Defence, Government of India. The Author is a Chevening Scholar from India and is currently pursuing M Sc. Global Security at UK Defence Academy. Email: amitsharma.drdo@gmail.com and asharma.dcmt@defenceacadamy.mod.uk .

Introduction

> "One hundred victories in one hundred battles is not the most skillful. Seizing the enemy without fighting is the most skillful."
>
> Sun Tzu Sixth Century B.C [1]

Sun Tzu in sixth century B.C. eloquently referred to the fact that, the best form of warfare is to take down the enemy without fighting with him.[2] Over time, as the warfare has evolved, this notion has gained impetus, especially with the genesis of cyberspace and cyber warfare. It was for the first time, that Sun Tzu's notion of, "Seizing the enemy without fighting is the most skillful" , could be imagined as happening in its entirety, using this potent new weapon which, in current contemporary world has no limits, no boundaries and to a surprise no visible restrictions or legislations. Although over time the notion of information warfare has matured and manifested into a form which has a colossal impact on how the contemporary wars are fought, but this has also resulted in the downgrading of strategic side of information warfare or cyber warfare to a decisive tactical force multiplier capable of turning the tides in war. Whilst this force enhancer aspect of cyber warfare is an important and decisive component of conventional warfare, but against the conventional wisdom this is not the end, but merely a beginning of the strategic aspect of cyber warfare.

In order to analyze the strategic aspect of cyber warfare, Luttwak's criteria of integration of a strategic warfare across all spectrum of affairs right from the tactical to the grand strategic level,[3] provides an important criterion for postulating the strategic framework for cyber warfare; Or in terms of Liddell-Hart, the coordination and assessment of means to achieve ends at all levels plays [4] a dominant role in casting a cyber warfare strategy. In light of these considerations, the author will elucidate the framework in which cyber warfare will have a strategic effect by acting as primary means to achieve conventional ends, hence will induce a paradigm shift from the conventional notion of cyber warfare as a tactical force multiplier to the notion of strategic cyber warfare acting as primary means of achieving grand strategic objectives in the contemporary world order. The author will accomplish this objective by deriving the elixir of Clausewitz's Trinitarian warfare and applying the concepts of Rapid dominance and Parallel warfare in cyber space so as to generate the strategic paralytic effect envisaged in effect based warfare. The author will conclude by shattering the conventional dictum of cyber defence, based on the notion of "defence in layers" and legal aspects of Law of Armed Conflict; by providing the only feasible and viable cyber defence strategy relying on the application of Rational Deterrence Theory (RDT) in general and on the idea of Mutually Assured Destruction (MAD) in particular so as to maintain the strategic status quo.

1. Cyber Irony- The Revolution in Military Affairs

Over last couple of decades, Information assets have had an irrefutable impact on the way, in which conventional wars are fought, to an extent that military theorists have termed it to be a Revolution in Military Affairs (RMA).[5] This extensive reliance of conventional warfare on information in contemporary conflicts is often misrepresented as information warfare rather than information-enabled warfare or information-enhanced warfare. The sudden significance ushered to this relatively new paradigm of information-enabled warfare, where information warfare is acting as a decisive force multiplier, has also raised certain existential questions for its survival predominantly that; whether this new paradigm of Information enabled warfare is really a strategic information warfare which will be the primary means of achieving ends or is it just a misinterpreted notion created by its loyal supporters, only to pacify the appetite of the change-hungry military world?

The answer to this existential question lies in the debate revolving around the notion, that information warfare is a revolution in military affairs. Alvin and Heidi Toffler have termed this information-enabled warfare as a third wave[6]; similarly most of the contemporary military theorists have termed this misinterpreted information warfare as a revolution in military affairs. At this juncture an important argument looms around the relation of a revolution in military affairs and its strategic effect. Throughout the history whenever there has been an occurrence of revolution in military affairs, it has always been followed with a strategic effect; for example revolutions in military affairs such as guns, artillery, airpower, nuclear weapons and so on, have always been accompanied with their strategic impact in creating a new world order. This important relationship between revolution in military affairs and its strategic effect is clearly missing in case of information warfare.

Hence if information warfare is really a revolution in military affairs then ideally it should have a strategic effect and since that effect is clearly missing, it can be concluded that something somewhere is missing. This gap is due to the misinterpretation of information warfare as mere decisive tactical information-enabled warfare acting as a force multiplier for conventional warfare. The Author believes that this notion is a fallacy; information warfare is more than just information-enabled warfare, which albeit represents an important aspect of information or cyber warfare, but not in totality. Cyber warfare is a strategic warfare which can be used as a principle means to achieve strategic ends and as required by Luttwak's criterion for strategic warfare [7], the framework for the strategic cyber warfare is to be defined across all spectrum of affairs right from the grand strategic to the tactical level.

2. The Grand strategic cyber warfare – the triad theory of cyber warfare

> "War is thus an act of force to compel our enemy to do our will"
>
> Clausewitz [8]

Clausewitz in his book *On War* clearly elucidated the fact that the end of the war is to compel the enemy to do your will [9] and Sun Tzu argues that the best form of warfare is the one in which the enemy is seized without a fight [10].Cyber warfare derives the essence of both of these great military theorists as it is a warfare which is capable of compelling the enemy to your will by inducing strategic paralysis to achieve desired ends and this seizing of enemy is done almost without any application of physical force.

Clausewitz formulated the theory of nature of war based upon the conception of Trinity. This elusive Trinitarian warfare according to Clausewitz held the key to victory in a war. Clausewitz predominantly constructed this trinity around three dominant tendencies, the blind force composed of primordial violence, hatred and enmity; the play of uncertainty and chance in which the creative spirit roams; and the reason for violence or the political instrument.[11] The tendencies are abstracted as, the people or the will to fight a war in terms of finances, manpower and support; the military or the means; and the government or the effort, the leadership and the direction which is essential for a nation.

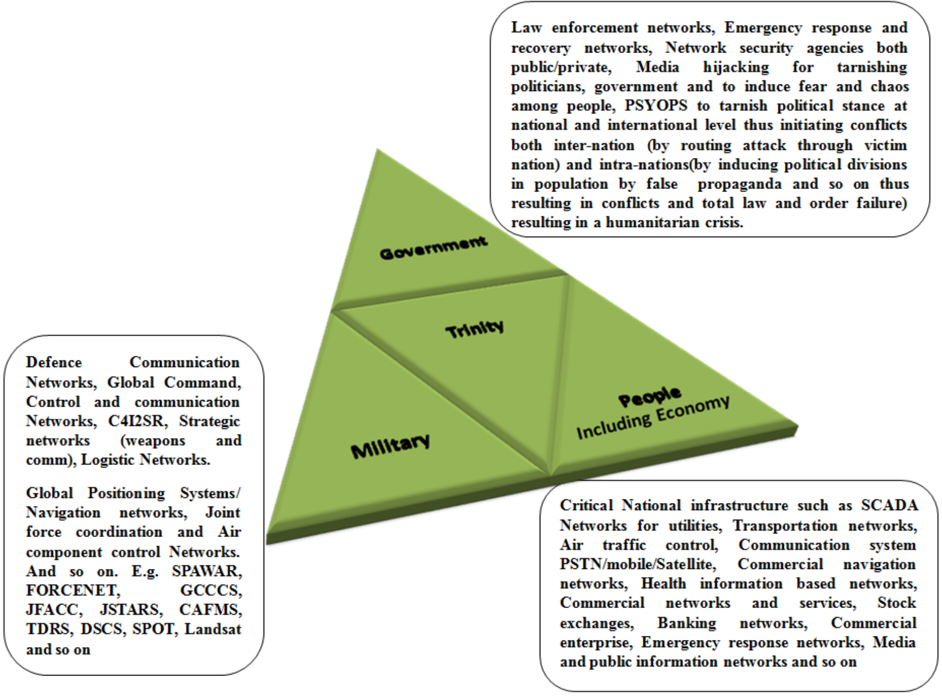
These three tendencies extensively interact with each other and have a continuously changing relationship. Till the time they are present and are interacting, the nation will sustain even when hit with the worse case scenarios. It is only when all of the three components are destroyed together or in conventional terms are subjected to parallel warfare; it is only then a 'cascade effect' will be generated to induce a strategic paralytic effect onto the Nation and the Nation as a system will crumble resulting in chaos and mayhem. In the current contemporary world in general and the developed countries in particular, the reliance on modern technology is not treated as a luxury, but a necessity where all the three tendencies are extensively dependent upon cyber space in one form or the other (Figure 1).

The modern militaries extensively depend on information assets and cyber space especially in scenarios where the deployment is across the globe. These information assets are used extensively in command and control systems especially in joint or coalition operations; in net-centric warfare operations involving global information grids; for logistic; for surveillance right from the information gathering which requires data links with satellites to information dissemination involving strategic information dissemination system; for communication right from the tactical field or theater data link operations and networks to strategic command and control networks involving communication satellites; global positioning and navigation satellites and networks for not only navigation, but for precision targeting; and so on(Figure 1).

The scenario is the same with the tendency involving the people or the will to fight a war in terms of finances, manpower and support. In almost all the developed countries and in some developing countries, people rely extensively on computers and cyber assets for almost all of their daily chores. Whether utilities such as gas and electricity; or health, transportation and banking facilities, all rely on cyber or network assets for their functioning. The scenario is even worse in case of banking and economic institutions like stock exchanges where money, which is nothing but numbers or information, travels across the national boundaries to the remotest corner of the world due to globalization of financial and banking instruments of economy. These technological advantages have not only eased the life of people, but have also made them vulnerable; as day by day people are becoming hopelessly dependent on these facilities to an extent that they take them for granted. The media and communication networks have almost become the vital sensory organs of this technologically dependent society.

This western society according to Bill Durodie is becoming more and more individualistic. It is becoming a society where people are socially disconnected; politically disengaged; and are in scientific disbelief.[12] In this society where perceptions overweight the reality, the people are becoming more and more 'risk averse' and are constantly living in an environment of fear. This state of society is classically defined by Ulrich Beck as a Risk Society.[13]

These societies are socially disconnected; politically disengaged; in scientific disbelief; and are constantly living in an environment of fear. The sudden disappearance of almost all of their facilities on which they are hopelessly dependent upon, will result in catastrophic outcomes where chaos, fear, bedlam, anarchy and basic animal instincts of man will prevail resulting in mayhem and complete destruction of nation as a system (Figure 2).



Law enforcement networks, Emergency response and recovery networks, Network security agencies both public/private, Media hijacking for tarnishing politicians, government and to induce fear and chaos among people, PSYOPS to tarnish political stance at national and international level thus initiating conflicts both inter-nation (by routing attack through victim nation) and intra-nations(by inducing political divisions in population by false propaganda and so on thus resulting in conflicts and total law and order failure) resulting in a humanitarian crisis.

Defence Communication Networks, Global Command, Control and communication Networks, C4I2SR, Strategic networks (weapons and comm), Logistic Networks.

Global Positioning Systems/ Navigation networks, Joint force coordination and Air component control Networks. And so on. E.g. SPAWAR, FORCENET, GCCCS, JFACC, JSTARS, CAFMS, TDRS, DSCS, SPOT, Landsat and so on

Critical National infrastructure such as SCADA Networks for utilities, Transportation networks, Air traffic control, Communication system PSTN/mobile/Satellite, Commercial navigation networks, Health information based networks, Commercial networks and services, Stock exchanges, Banking networks, Commercial enterprise, Emergency response networks, Media and public information networks and so on

Figure 1: The notion of trinity in terms of strategic cyber warfare. (Source: Author)

The third and the most dominant tendency constitute the government, the political instrument and the leadership. Government plays an important role in providing leadership to the nation and in combining efforts and means to achieve political aims; hence for the failure of nation as a system, it is important that along with the other two tendencies the political instrument should also be destroyed.

In current contemporary world, governments play as the political instrument in the trinity by means of excising control and gaining the mandate of people. These objectives are achieved by using effective law enforcement and by providing a secure, secular and democratic environment to people to attain control and mandate over them. The law enforcement and security agencies rely extensively on criminal records and other coordination networks such as emergency response and recovery networks which although act as a force multiplier for them, but at the same time make them vulnerable to strategic cyber warfare. Another important aspect to gain mandate and control of people is the media. Media is an important tool that frames the perception and psychological frame of mind of the population. The 'CNN effect' is a potent tool to influence the mindsets of people.[14] Media around the world is extensively interlinked through networks which not only makes information to disseminate easily, but also make media more susceptible to strategic cyber warfare. These Media networks can be hijacked for tarnishing the image of politicians and the government of a victim nation; and can be used to induce fear and chaos among people. PSYOPS can be fully employed on these hijacked media networks to tarnish the political stance of the victim nation at national and international levels, thus initiating conflicts both at inter-nation level (by routing an attack through a victim nation) and intra-nation level (by inducing political divisions in the population by false propaganda and so on, thus resulting in conflicts and total law and order failure), hence creating the symptoms of a failed state which has anarchy, fear and chaos, resulting in a humanitarian crisis and failure of the state (Figure 2).

As described above, these three tendencies form the core of a nation or constitute the nation as a system of systems. All of these components are quite resilient in nature unless and until they are simultaneously attacked and destroyed, they are quite capable of reviving one another. Thus in order to achieve a strategic effect and to gain rapid dominance, parallel warfare should be initiated in cyber space so as to destroy all the three tendencies simultaneously (Figure 2). The Author believes that the cyber attacks such as *Titan Rain; attacks on Estonia and Georgia;* and so on were not successful due to the fact that they were tactical in nature and were targeting the individual components of the trinity at a time. Since these components are resilient when they are together, so even if one of the tendencies is fully destroyed in a cyber attack, the other two tendencies will tend to rescue it, hence a strategic paralytic effect will not be achieved. The author believes that it is for this reason the cyber attacks conducted so far could not achieve a strategic effect and were ineffective.

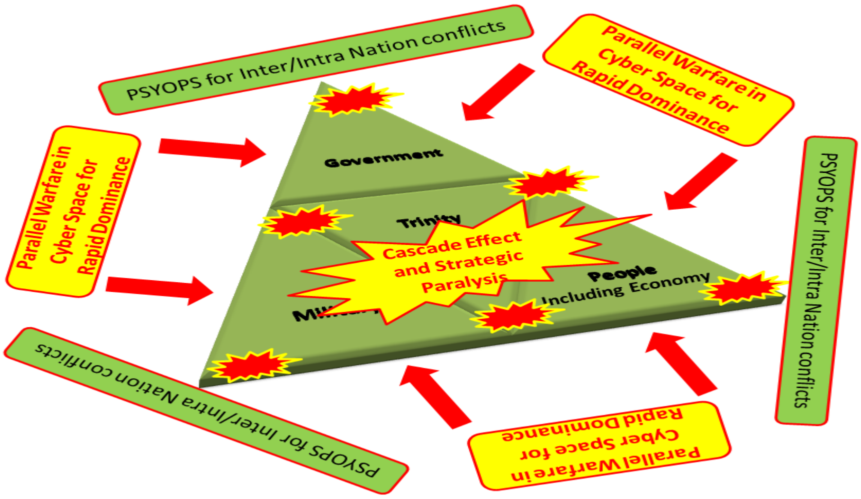

PSYOPS for Inter/Intra Nation conflicts
Parallel Warfare in Cyber Space for Rapid Dominance
Parallel Warfare in Cyber Space for Rapid Dominance
PSYOPS for Inter/Intra Nation conflicts
Government
Trinity
Cascade Effect and Strategic Paralysis
People
Including Economy
Mi
PSYOPS for Inter/Intra Nation conflicts
Parallel Warfare in Cyber Space for Rapid Dominance

Figure 2: Cyber Trinity based parallel cyber warfare attack to induce strategic paralytic effect on a victim nation (Source: Author)

In order to achieve a strategic paralytic effect via the application of cyber warfare, all the three components of the trinity should be attacked simultaneously. These cyber attacks should be performed by using the paradigm of parallel warfare[15], which relies on gaining rapid dominance by producing the desired effect of paralyzing the control of the enemy by performing rapid decisive operations at all levels i.e. the strategic, operational and tactical; across the spectrum involving related assets and critical components of all the three tendencies of the cyber trinity; and with rapid succession so as to reduce the chances of counter attack or of the “defensive phenomena” of *pulling the plug.*

When the art of simultaneous parallel warfare to achieve rapid dominance is combined with the strategy to simultaneously attack the three components of the cyber trinity, it will generate a *cascade effect* rendering the victim in a paralytic state with the loss of control over the state and failure of the state-as-a-system, thus generating ramifications which are way ahead than mere arithmetic benefits generated by a successful attack. This failure of Nation as a system-of-systems and the disruption or paralysis of the state will destroy the victim’s will and capability to fight thus ‘compelling it to submit to your will’.

This strategy of strategic cyber warfare against the Trinity in cyber space to achieve strategic paralysis provides for an alternative warfare or means to achieve strategic effect of rendering the enemy ineffective to operate as per its wishes, eventually is more important than the conventional paradigm of destruction-based warfare to annihilate the forces it depends upon for its defence, hence generating not only a strategic victory, but also a constructive conflict termination. This constructive conflict termination is not only desired, but is imperative especially in the contemporary world, with examples of conflicts with flawed exit strategies resulting in victories turning into protracted wars such as the Iraq war.

3. Campaign planning- The orchestration of strategy

Once the strategy for conducting cyber warfare to achieve the strategic end of compelling the enemy to submit to your will by rendering the enemy ineffective is defined, the next important task is to integrate that strategy to a campaign plan which spreads across all levels of warfare. This process of accessing the assets and means to achieve the desired effect and ends by orchestrating the strategy across all levels of warfare is termed as the campaign planning and the scenario is the same in pursuing a strategic cyber warfare campaign.

As done in conventional warfare the campaign planning for strategic cyber warfare is also based on phasing, but against the conventional dictum of executing these phases in sequential or near sequential manner, the strategic cyber warfare tends to use these phases in almost near parallel manner. At any temporal instance, each of the phases will have a substantial effect over the entire theater of operations in general and individual zones in particular in conformance with the parallel warfare dictum. When applied in order to orchestrate the strategic cyber warfare strategy of generating a paralytic effect on the adversary by initiating parallel cyber attacks on all the three components of the Trinity, all phases of the campaign will overlap extensively and the campaign will be in the form of simultaneous waves of these overlapping phases tailored according to the theater conditions at all levels.

The campaign for strategic cyber warfare in line with conventional dictum[16] will consist of five broad stages; Shape, Deter, Seize initiative, Dominate and Exit (Figure 3). Out of these the Shape and Deter are part of the pre conflict phases; Seize initiative and Dominate are usually the conflict phases; and the Exit is the post conflict phase. Although these phases are lucidly categorized as pre-conflict; conflict; and post-conflict phases, these categorizations tend to overlap extensively. For example even though there would be a conflict in progress in certain parts of the theater, but still in certain other parts, the Shape and Deter phases may be exercised to limit the conflict from further escalation.

The initial phase or the Shape phase revolves around shaping the conflict.[17] This is done using extensive peacetime cyber reconnaissance, such as mapping enemy's or potential adversary's cyber assets, network design, layout, vulnerabilities, critical components and dependence; assessing enemy's cyber defence capabilities both offensive and defensive; boosting national cyber defence capabilities not only in military, but in all the components of the cyber trinity; identification of critical assets/targets which would initiate a 'cascade effect'. In order to identify these components the 'Critical component theory' which was utilized by the allied air force for strategic bombing of Germany during the Second World War[18] can prove an important asset, And performing all the above operations on your own assets also, can be useful to identify potential susceptibility and vulnerabilities.

Apart from cyber reconnaissance, an important component included in the peacetime operations involves the process of inducing vulnerabilities in enemy's cyber assets. This is achieved either by using cyber means such as installing covert malware such as trojans, rootkits, dormant stealth malware and so on; or by using covert means such as exporting bugged firmware by using front door companies, thus making enemy systems susceptible to Permanent Denial Of Service (PDOS) attacks and by covertly gaining information of enemy's critical system software such as operating systems, by gaining access to the skeleton keys for the backdoors, usually channeled through vendor influence; and so on.

Deter like the Shape phase is also a pre-conflict phase which extensively revolves around shaping the future conflict by gaining a credible and known deterrence. This phase capitalizes on the information gained during the cyber reconnaissance of the adversary's and of personal cyber infrastructure and their susceptibility to strategic cyber attack. Based upon this information, relevant steps are initiated to harden personal infrastructure in terms of 'layers of defence' and redundancy; and to prepare for exploiting the enemy's vulnerabilities and then testing them in simulated environments by conducting cyber war games.

An important part of this phase is to develop a cyber deterrence which is credible and is made known to the enemy. The credibility of the cyber deterrence can be achieved by creating a *Cyber Triad capability*, equivalent to a *Nuclear Triad*[19] which will have capability for orchestrating a second strike in case of failure of the deterrence. Cyber Triad capability can consist of Regular defence/military assets and networks as forming the first section of the triad; the second section of the triad can consist of an isolated conglomerate of air-gapped networks situated across the friendly nations as part of cooperative defence, which can be initiated as credible second strike option; and the third section of the triad can consist of a loosely connected network of cyber militia involving patriotic hackers, commercial *white hats* and private contractors which can be initiated after the initial strike or in case of early warning of a potential strike. This Cyber Triad creates a scenario of a credible and undisputable cyber deterrence and second strike capability thus assuring a *Mutually Assured Destruction (MAD)* in cyber space.

The later feature of the cyber deterrence involving the policy of making the cyber deterrence known to the enemy, can be achieved by following a 'cyber countervailing' strategy in line with the 'countervailing' nuclear strategy followed by NATO forces during the cold war.[20] This strategy revolved around making known to the potential adversary that the implication of a nuclear strike would be far greater than the potential gains an adversary can achieve by initiating the first strike. The scenario will remain the same in the strategic cyber warfare where the potential enemy should be made known of the potential risk it might be facing in light of initiating a first strike. This can be achieved by means of media coverage; extensive war games; and to some extent by covert instantiation of limited cyber warfare attacks on the adversary. The author believes that the recent attacks such as the Titan Rain; the attacks on Estonia and Georgia; and attacks on various other countries around the world such as UK, France Germany, India and so on; can be a part of a *cyber countervailing strategy.*

Once the conflict has been initiated there can be two possibilities; either the cyber deterrence has failed and the enemy has initiated the first strike or due to certain unforeseen events, friendly forces needed to initiate the first strike. In the former situation it should be always assumed that the adversary's first strike will have, if not an all out decapitating effect, a certain degree of effect on friendly cyber infrastructure, but an important aspect here is to detect the attack before it could generate any strategic paralytic effect. Once this detection is achieved, it is required that necessary steps should be taken so as to activate the cyber triad to initiate the second strike capability. This can be achieved by taking defensive counter measures and securing cyber infrastructure; initiating the second triad involving a coordinated and real-time integration of an isolated conglomerate of air gapped networks situated across friendly nations as part of cooperative defence; and in a worst case scenario, where there is a total loss of offensive and defensive capabilities, the third component of the triad consisting of a loosely connected network of cyber militia involving patriotic hackers; commercial *white hats* and private contractors should be activated in order to initiate a protracted conflict. This protracted conflict is essential to gain time so as to revitalize your own capabilities in worst case scenarios.

Similarly if the first strike is to be initiated, the primary aim should be on the total destruction of the cyber triad. This is done so as to destroy enemy's capability of retaliation and to provide strategic freedom of operation in cyber space to friendly forces. This strategic freedom of operation in cyber space is essential in order to initiate the strategic cyber warfare on the critical components of the cyber trinity for achieving the strategic paralytic effect. An important consideration at this point should be on the fact that these phases should be conducted in an overlapping fashion to perform parallel warfare in cyber space.

Once the necessary objectives are achieved and the desired end-state is reached due care should be taken to stabilize the situation. Although the effects of strategic cyber warfare like the nuclear warfare are far reaching, devastating, and in a way cannot be measured, they still can be contained and the post-conflict situation can be stabilized by initiating external support in the form of reestablishing the cyber services and facilities and retrieving of data, if not fully, then to a decent level, so as to carve out an exit strategy. Like in conventional conflicts, the chances of a cyber insurgency consisting of patriotic hackers and of humanitarian crisis loom at large especially in a post-conflict scenario. Hence due care should be taken to reestablish the essential services and command and control infrastructure after the conflict. An aggressive media strategy to counter dissident feeling and anguish among the people should be utilized so as ease the stabilization process and assist with post conflict rehabilitation.

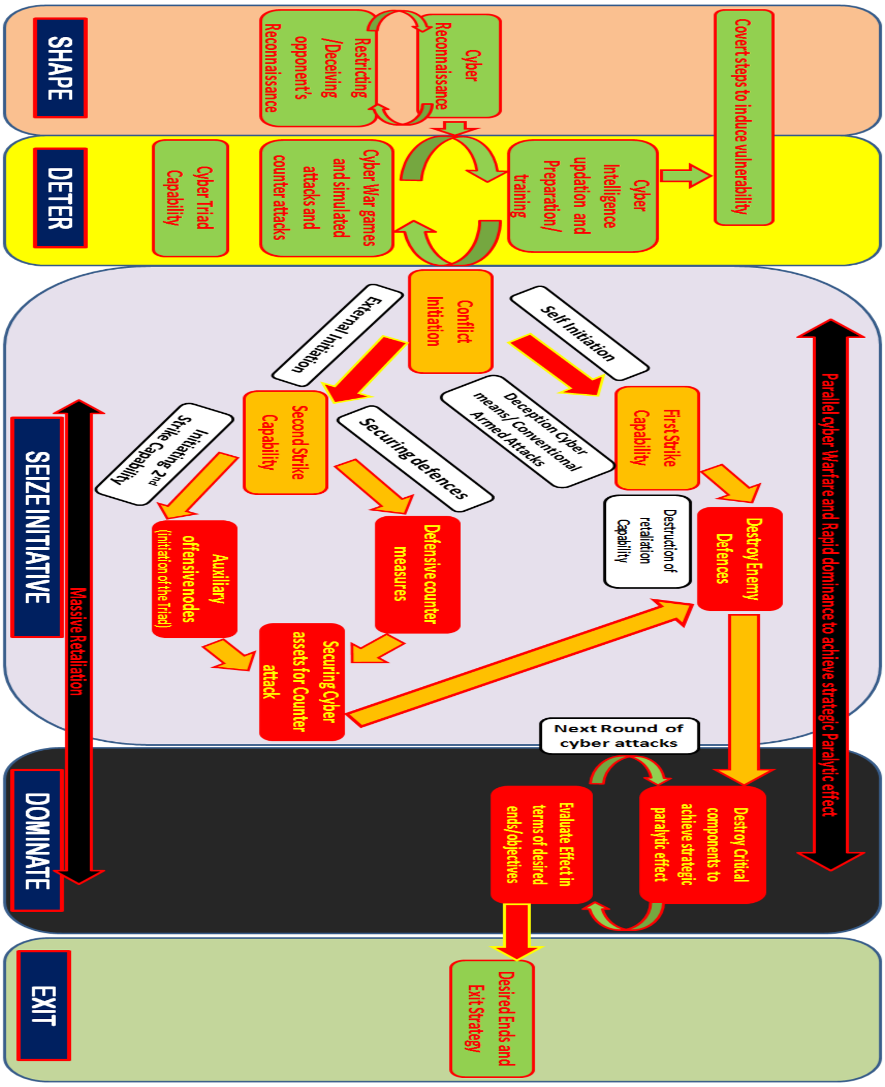

SHAPE
DETER
SEIZE INITIATIVE
DOMINATE
EXIT
Cyber Reconnaissance
Restricting /Deceiving opponent's Reconnaissance
Covert steps to induce vulnerability
Cyber Intelligence updation and Preparation/ training
Cyber War games and simulated attacks and counter attacks
Cyber Triad Capability
Conflict Initiation
Self Initiation
External Initiation
First Strike Capability
Second Strike Capability
Deception Cyber means/ Conventional Armed Attacks
Securing defences
Initiating 2nd Strike Capability
Auxiliary offensive nodes (Initiation of the Triad)
Defensive counter measures
Securing Cyber assets for Counter attack
Destroy Enemy Defences
Destruction of retaliation Capability
Massive Retaliation
Parallel cyber Warfare and Rapid dominance to achieve strategic Paralytic effect
Next Round of cyber attacks
Destroy Critical components to achieve strategic paralytic effect
Evaluate Effect in terms of desired ends/objectives
Desired Ends and Exit Strategy

Figure 3: Cyber campaign planning for strategic cyber warfare. (Source Author)

4. Cyber Defence – A conventional fallacy

The current conventional wisdom on cyber defence relies on the notion of 'defence in layers'[21] and on International legal regulations especially by drawing similarities between cyber attacks and armed conflicts and then applying the law of armed conflict [22] appropriately. The notion of 'defence in layers' is a tried and tested dictum which is extensively used to protect both the commercial and the defence networks. It relies on installing multiple layers of defences so as to make the penetration almost impossible. Even though this notion has extensively been used to protect cyber infrastructure, it is a known fact that such a system is as strong as its weakest link. No matter how much the system is hardened and no matter how many layers are used to secure the system, there is still no guarantee that the system security is foolproof. It is safe only up until the time when someone doesn't find any vulnerability or an exploitable construct in the system, which can be exploited to gain access in to the system. Yes, this notion of defence at least assures that the penetrator will require time to defeat multiple layers of security. It is this time that is crucial for defenders to take necessary action to thwart the threat. Hence this provides for a minimum deterrence, but nevertheless is not a complete and foolproof solution.

The other aspect of conventional wisdom on cyber defence relies on the legal framework of international law both *jus ad bellum* and *jus in bello*. This defensive strategy relies on the deterrence generated by the legal punitive aftermath of a cyber conflict on the erring side. The notion relies extensively on drawing similarities between the conventional international armed conflicts and cyber conflicts; and then applying the international laws which will fit the scenario. Most of the discussion in this realm revolves around self defence for *jus ad bellum* and Law of armed conflict for *jus in bello*. Extensive analysis is done in order to find the lines of similarity between the armed conflicts and cyber attacks, but these arguments in a sense degrade the strategic aspect of cyber warfare to mere tactical cyber attacks or are centered towards the means rather than the strategic ends.

The author believes that this notion of defence is a fallacy as the underlying assumption of treating strategic cyber warfare as mere tactical cyber attacks is in itself a fallacy. If cyber warfare is performed so as to achieve the strategic paralytic effect, then the consequences of such a warfare would be far reaching and to an extent not measurable in conventional terms. The *cascade effect* initiated as an aftermath of strategic cyber warfare would generate a chain of 'unintended consequences' that are almost impossible to tackle using the conventional framework of law of armed conflict. The only appropriate legal frame work to handle strategic cyber warfare would be based on the legal frame work of *jus ad bellum* and *jus in bello* for nuclear weapons, which unfortunately is a long debated notion and has an incoherent international opinion visible extensively in the ICJ's opinion [23] over the use of nuclear weapons.

In light of these circumstances, where the conventional dictum of cyber defence is a mere fallacy the only viable and achievable option for cyber defence would rely on the age old dictum of deterrence and to an extent on the cold war principle of Mutually Assured Destruction. This cyber deterrence can be guided by the Rational Deterrence Theory (RTD) which relies on the underlying assumption of actors to be rational and performing cost benefit analysis before reaching any logical conclusions; and the outcome variation depends upon the variations of opportunities which the antagonists have.[24] Ashen and Snidal argue that the key concepts for achieving deterrence based on RDT will be on the credibility of the deterrence capabilities and the rational actor assumption of decisions relying on cost benefit analysis.[25] In terms of cyber deterrence the credibility can be achieved by the creation of a cyber triad as part of the Deter phase of cyber campaign planning. This cyber triad capability can consist of Regular defence/military assets and networks as forming the first section of the triad; the second section of the triad can consist of an isolated conglomerate of air-gapped networks situated across the friendly nations as part of cooperative defence; and the third section of the triad can consist of a loosely connected network of cyber militia involving patriotic hackers, commercial *white hats* and private contractors

This credible second strike capability assures the dictum of Mutually Assured Destruction (MAD) in cyber space and hence an option for defence in terms of deterrence. This capability should be made known to the potential advisories as part of cyber *countervailing* strategy to warn them of undesired consequences and punitive costs they may bear in the event of a cyber conflict. This form of deterrence is generally classified as the *deterrence by punishment*; the other form of deterrence is classified as the *deterrence by denia*l.[26] This deterrence by denial in cyber defence can be achieved by preemptive cyber strikes on the adversary's cyber offensive capabilities. However, in scenarios of state actors this policy may result in a further escalation of conflict; hence utmost care and thought process in regard to attribution of cyber attacks should be taken before initiating such a strike. In the case of non-state actors the *deterrence by denial* in the form of preemptive cyber strikes, offer a credible deterrence mechanism for thwarting any such threat. In both the scenarios, extensive reconnaissance and surveillance both by cyber and conventional means can act as suitable tools for attribution and target selection.

It follows that cyber deterrence can act as an important means for thwarting both the state and non-state threats by means of *deterrence by punishment* and *deterrence by denial*. Also it is clearly evident that none of the cyber defence notions can provide for a holistic cyber defence; hence a cyber defence strategy should be a combination of the notion of 'defence in layers'; the legal aspects of International law, although whether the Law of Armed conflict may be applicable in its entirety is debatable, but that is out of the scope for this article; and by generating a credible cyber deterrence based on the cyber triad, thus assuring a Mutually Assured Destruction in cyber space and hence a strategic status quo.

5. Cyber finale

The last couple of decades have seen a colossal change in the way in which conventional wars are being fought, with information being an integral component. Information and information assets have made such an indelible impact on warfare that military pundits often misinterpret this information-enabled warfare to be information warfare, where information assets act as decisive force multipliers, which are capable of changing the outcome of wars. Although it is a considerable feat, but in a sense it degrades the strategic aspect of information warfare to mere tactical cyber attacks. Over years this paradigm of considering information warfare as mere tactical force multiplier has gained impetus. This paradigm has created an environment where "means are emphasized more than the desired ends". The author believes that this is a fallacy and calls for a paradigm shift from "means to ends". The Information warfare is a strategic warfare which derives the essence of both Sun Tzu and Clausewitz as it is a type of warfare which is capable of compelling the enemy to do your will by inducing strategic paralysis to achieve desired ends and this seizing of the enemy is done with virtually no application of physical force.

The strategic information warfare is capable of achieving desired strategic ends by inducing a strategic paralytic effect onto the nation; and the nation as a system will crumble resulting in chaos and mayhem. This strategic effect relies on the framework defined across all spectrum of affairs, right from the grand strategic to the tactical level, and is achieved by the strategy of strategic cyber warfare against the Clausewitz's Trinity in cyber space to achieve strategic paralysis and rapid dominance using parallel warfare. This strategy provides alternative means to achieve the strategic effect of rendering the enemy ineffective to operate as per its wishes, which eventually is more important than the conventional paradigm of destruction-based warfare to annihilate the forces, the enemy depends upon for its defence; hence generating not only a strategic victory, but also a constructive conflict termination.

In order to achieve these ends, a comprehensive orchestration of strategy in the form of campaign planning is required, which in line with conventional dictum will consist of five broad stages; *Shape, Deter, Seize initiative, Dominate and Exit*; categorized further as pre-conflict, conflict and post-conflict phases. Out of these the most crucial are the pre-conflict phases of Shape and Deter, which involve extensive cyber reconnaissance and the creation of a credible and known cyber deterrence based on *cyber triad* capability and *cyber countervailing strategy*. This creates a credible second strike option in cyber space, which assures a strategic status quo based on Mutually Assured Destruction in event of a cyber conflict.

In terms of cyber defence the conventional wisdom of treating of cyber warfare as mere tactical cyber attacks or force multipliers and relying on the legal framework of Law of Armed Conflict (LOAC) for defence is a fallacy; as it not only undermines the strategic aspect of cyber warfare in the form of generating strategic paralytic effect to achieve political ends, but it also relies on a legal framework for defence, which is contemplated on a false assumption of drawing similarities with conventional armed conflicts. The only warfare which matches cyber warfare in strategic terms is nuclear warfare; and as there is a gross division of International Law in terms of *Jus ad bellum and jus in Bello* for Nuclear weapons, the scenario unfortunately will remain the same for cyber warfare also.

Under these circumstances, the only feasible and viable cyber defence strategy will rely on the application of Rational Deterrence Theory in general and on the idea of Mutually Assured Destruction in particular so as to maintain the strategic status quo. Hence the author recommends that the nations should reconsider their cyber defence strategies, and should define a strategy based on a combination of the notion of "defence in layers"; legal instrument; and potent cyber triad based cyber deterrence. This would be the only viable and achievable option in current contemporary and futuristic conflicts, which the author predicts, will be dominated by strategic cyber warfare as the "primary means to achieve strategic ends".

References

[1] Sun Tzu translated by Samuel B. Griffith, *The Art of War*. (Oxford University Press, 1963).

[2] Sun Tzu translated by Samuel B. Griffith, *The Art of War*. (Oxford University Press, 1963).

[3] Luttwak Edward, Strategy: The Logic of War and Peace, (London: Harvard university press, 1987).

[4] Liddell Hart Basil Henry, *Strategy,* (New York: Meridian, 1991).

[5] Charles A. Ray, "Cyber war and Information Warfare: A Revolution in Military Affairs or Much Ado about Not Too Much?", National War College Report, 1997.

[6] Alvin and Heidi Toffler, The Third Wave- The Classic Study Of Tomorrow, (Bantam Books,1980)

[7] Luttwak Edward, Strategy: The Logic of War and Peace, (London: Harvard university press, 1987).

[8] Michael Howard and Peter Paret, eds., On War (Princeton University Press, 1984) Book I, Chapter 1, section 2, pp 75.

[9] Michael Howard and Peter Paret, eds., On War (Princeton University Press, 1984) Book I, Chapter 1, section 2, pp 75.

[10] Sun Tzu translated by Samuel B. Griffith, *The Art of War*. (Oxford University Press, 1963)

[11] Michael Howard and Peter Paret, eds., On War (Princeton University Press, 1989) pp 583.

[12] Bill Durodie, "The Limitation of Risk Management" , *TIDSSKRIFTET POLITIK* ,Vol. 8 No.1,2004.

[13] Ulrich Beck, *Risk Society: Towards a New Modernity*, (New Delhi: Sage, 1992).

[14] Belknap, Margaret H. *The CNN Effect: Strategic Enabler or Operational Risk?,* U.S. Army War College Strategy Research Project. 2001.

[15] Deptula David, *Firing for Effect: Change in the Nature of warfare,*(Arlington: Aerospace Education Foundation,1995).

[16] Joint Publication 3-0 *Doctrine for Joint Operation,* December 2005,IV-34.

[17] Joint Publication 3-0 *Doctrine for Joint Operation,* December 2005,IV-34.

[18] Pape Robert, *Bombing to Win: Airpower and coercion in war*,(Ithaca: Cornell university press,1996).

[19] Aldridge Robert C, First strike!: the Pentagon's strategy for nuclear war,(Cambridge: South End press,1983)

[20] Powell Robert, "Nuclear Deterrence and the Strategy of Limited Retaliation", *The American Political Science Review*, Vol. 83, No. 2 (Jun., 1989), pp. 503-519

[21] Harold F. Tipton and Micki Krause, *Information Security Management Handbook,* (Florida: CRC Press, 2006).

[22] Matthew E. Haber, Computer Network Attack and the Laws of Armed Conflict: Searching for Moral Beacons in Twenty-First-Century Cyber warfare, ARMY Command and general staff college, Fort Leavenworth, 2002.

[23] The 1996 ICJ's opinion over the Legality of Nuclear Weapons.

[24] Achen, Christopher and Snidal Ducan," Rational Deterrence Theory and comparative case studies", *World Politics*, Vol. XLI, No. 2, pp.139-169.

[25] Achen, Christopher and Snidal Ducan," Rational Deterrence Theory and comparative case studies", *World Politics*, 1998, Vol. XLI, No. 2, pp.139-169.

[26] Downs George," The Rational Deterrence Debate", *World Politics*, 1998, Vol. XLI, No. 2, pp.225-237.