EXPLAINING WAR AND PEACE IN INTERNATIONAL RELATIONS: A STUDY OF OFFENCE-DEFENCE THEORY

Dissertation submitted to Jawaharlal Nehru University in partial fulfilment of the requirement for the award of the degree of

MASTER OF PHILOSOPHY

SHALINI PRASAD

JNU

Diplomacy and Disarmament Division,
Centre for International Politics, Organisation and Disarmament
School of International Studies
Jawaharlal Nehru University
New Delhi- 110067

2011

Centre for International Politics, Organization and Disarmament

Date: 25/7/11

DECLARATION

I declare that the dissertation entitled **"Explaining War and Peace in International Relations: A Study of Offence-Defence Theory"** submitted by me for the award of the degree of **MASTER OF PHILOSOPHY** of Jawaharlal Nehru University is my own work. The ~~thesis~~ dissertation has not been submitted for any other degree of this University or any other university.

Shalini Prasad
SHALINI PRASAD

CERTIFICATE

We recommend that this dissertation be placed before the examiners for evaluation.

25.7.11
Prof. SWARAN SINGH
Chairperson CIPOD

Centre for International Politics,
Organization & Disarmament
School of International Studies
J.N.U., New Delhi

J Madhan Mohan
Dr. J.MADHAN MOHAN
Supervisor

Dedicated

To

My Family

For Their Consistent and Invariable Support

Contents

Acknowledgement

First and foremost I would like to thank and express my heartiest gratitude to my supervisor Dr. J Madhan Mohan for his guidance and insightful suggestions. This work would not have been possible without his illuminating inputs at regular intervals. His professional excellence contributed greatly towards shaping the research.

I would like to take this opportunity to thank the faculty members of CIPOD, especially Prof. Swaran Singh, Prof. Pushpesh Pant, Prof. Rajesh Rajagoplan, Prof. Amitabh Mattoo, Dr. Moushmi Basu, and Manish Dhabade for sharing their valuable which was extremely important in making this research fruitful. I express my gratitude to the Library Staff of the Jawaharlal Nehru University, Institute for Defence and Analysis (IDSA) and United Services of India (USI).

This work is in its current shape because of the sincere and dedicated efforts of my friends, especially Abhay Kumar, Preeti Gupta, Anjum Shaheen M.P Shibu, Padmam and Holi Ayemi. It is not possible to mention each and every name here and so I would like to thank everyone who helped me in this endeavour.

Last but not the least, I would like to thank my respected parents and other members of my family. Their contribution was a rare source of moral inspiration was of constant support.

Shalini Prasad
Shalini Prasad

ABBREVIATIONS

ABM	:	Anti Ballistic Missile
ATM	:	Automated Teller Machine
COMINT	:	Communication Intelligence
CIA	:	Central Intelligence Agency
ELNIT	:	Electronic Intelligence
FBI	:	Federal Bureau of Investigation
GII	:	Global Information Warfare
GNP	:	Gross National Product
ICBM	:	Intercontinental Ballistic Missile
IW	:	Information Warfare
MAD	:	Mutual Assured Destruction
MIRV	:	Multiple Independently Targetable Restricted Vehicle
NFU	:	No First Use
OBD	:	Offence Defence Balance
SIGNIT	:	Signal Intelligence
SATAN	:	Security Administration Tool for Analysing Networks

Chapter One

Introduction

Introduction

The purpose of the study is to analyse the explanatory power of offence-defence theory. This theory seeks to explain war and peace in international relations. The study proceeds by examining the role of technology in offence-defence balance in three phases. The first phase deals with conventional warfare which mainly signifies the pre -nuclear age. The second phase denotes the period after the end of the Second World War which is interpreted as the nuclear era. The third phase will examine the period of information warfare by elaborating on the relevance of offence-defence theory.

Offence-Defence theory has been propounded by various scholars through different perspectives. Robert Jervis, Stephen Van Evera, Charles Glaser, Jack Levy and Chaim Kauffman deserve special mention. The theory rests on an important parameter, *i.e.* offence-defence balance. Jervis, one of the proponents of offence-defence theory, makes the prediction that international conflict and war is more likely when offence has the advantage while peace and cooperation is more probable when defence has the advantage. He further argues that war in which offence has the advantage further increases the security dilemma. War would in turn become profitable in the offensive advantage while if there is defensive advantage, the situation would be reversed. Small and weak states could form alliances and deter the attack by raising the costs of conquest (Jervis 1978).

Jervis also focuses on the differentiation between offensive and defensive weapons. It means that the weapons which are used for defensive purposes could also be used for attack. The differentiation between offensive and defensive weapons could be analysed at the level of defensive strategies. Fortifications that can shelter forces and attack can be kept under the purview of defensive weapons as the meaning of defensive weapon is to protect the territory without being able to penetrate into enemy land. On the other hand, weapons that are particularly offensive are inclined to destroy the fortifications and used in strategies for surprise attack (Jervis 1978).

Further, this theory not only categorises any individual weapon as offensive or defensive but also focuses on the deployment of weapons. If deploying the weapon shifts the balance towards offence, then it would be an offensive strategy. Technology is the major determinant which shapes the offence- defence balance. It influences the state's power and determines the offensive and defensive strategy (Jones 1995). The core theory offers the basic criteria for judging how a given technology affects the offence-defence balance and thus military outcomes: mobility-improving innovations generally favour offence and result in a quick and decisive victory for the attacker, whereas power-enhancing innovations typically strengthen defence and lead to more indecisive warfare. Stephen Van Evera argues that military technology largely impacts on the offence-defence balance *i.e.* technologies that favour offence advantage tend to be offensive and vice versa. He had compared different weapons in conventional warfare and examined how technology influences the states to adopt offensive and defensive strategies (Evera 1998).

Offence-defence balance theory can be analysed in three phases. The first is conventional warfare, the second pertains to nuclear era and the third phase denotes the current phase of information warfare. The conventional warfare, which indicates the pre-nuclear era, demonstrates that advances in explosives technologies determined the offence-defence balance. Proponents of offence-defence theory believe that new or improved technologies that enhance mobility contribute relatively more to offence than defence. In military terms, mobility is the ability of troops and equipment to move from one place to another. Strategic mobility is the ability to transport military forces from the home or land to a theatre of operations, or from one theatre to another. Offence-defence theorists argue that greater strategic mobility allows the attacker to expeditiously transport and supply its forces far from its own borders, thus negating the defender's geographic advantage (Glaser and Kauffman 1998).

During the period of First World War, lethal small arms, barbed wires and trenches gave defenders a large advantage at the point of attack. However, in the later period, the power of the offence was restored by 'motorised armour' (Evera 1998). Technology influences the swift of offence and defence balance. In the conventional warfare period the balance tends to shifts sometimes towards offence and defence and *vice versa*. So it cannot be classified as offence dominant or defence dominant but a continuum process where offensive and defensive strategies both rule the politics of peace and war in international politics.

Offence and defence theory also played a central role in the development of nuclear weapons theory. Proponents of offence-defence theory argue that the nuclear revolution strongly shifted the offence-defence balance toward defence. In the nuclear era, wherein both sides can simultaneously gain security in the form of second strike capability, there is no incentive to strike first in a crisis (Jervis 1998). The only way is to eliminate the second strike capability which is very difficult because it is much easier to build up own arms rather than to strengthen the forces that threaten adversary's deterrent forces (Lieber 2000).

The characteristics of nuclear weapons, with their enormous power indicates that the first strike capability is hard to attain while a second strike capability is easy to be applied. As a result, the balance is shifted towards the defence side when not only the great powers are unconquerable but even lesser powers could stand stronger against aggression (Evera 1998).

After the 11 September 2001 attack, conflicts in international relations became more intense. This is the age of information warfare. The purpose of information warfare is to disable an enemy's defence, to gain information, to disrupt infrastructure and to reduce the will to fight. The advantage of cyber warfare is that an attack may be performed from a great distance, at the speed of light and at the click of a button. An attack that prevents attribution hides the source of the attack. Hiding the source hides the responsibility, preventing legal recourse or targeting for counter attack. In cyber threat, it is difficult to determine as to who launched the attack.

Cyber warfare could be termed as offence-dominant because the internet or the defender technology is not fully aware of the source and the origin of the threat is transparent and encourages ease of technical innovation. Structurally, it could be found that the defender is always lagging behind the attacker in terms of developing measures and countermeasures. Information technology is spreading into nearly all military weapons, communications, and command and control systems, as well as the civilian systems that support modern industrial (or post-industrial) economies and their military efforts. As such, information warfare includes both new techniques, such as computer infringement and disruption.

The theory of offence-defence balance has been dealt in detail in a wide array of academic works. Almost all the existing literature on the theme used the theory to analyse war and peace in international relations. There seems to be a general consensus regarding the significance of technology in offence-defence theory. Most of the works agree on the prediction that international conflict and war is more likely when offence has the advantage while peace and cooperation is more probable when defence has the advantage. Jervis (1978) explained the variables of offence and defence balance. Distinction needs to be drawn between offensive and defensive weapon and whether defence or the offence has the advantage. When there are incentives to strike first, the state would desire for attack as victory is more or less decisive. When the defence has the advantage, the strategy would be reversed. The essence of defence is keeping the other out of one's territory. A purely defensive weapon can do this without being able to penetrate state's enemy land. The most obvious example he cited is fortification. He defined offensive weapons as those which are effectively used in reducing defensive operations. For example, mobile artillery is denoted as offensive weapons as it is used in destroying fortifications.

Evera (1998) explained that war is far more likely when conquest is easy, and the shift in the offence-defence balance impacts the risk of war. According to him, technology alone does not determine the offence-defence balance. Military technology and doctrine, geography, national social structure and diplomatic arrangements, specifically defensive alliances, impact upon offence-defence theory. In essence, offence-defence balance is an aggregate of these geographic, social and diplomatic factors. He provided ample explanations to make a distinction between offensive and defensive weapons. He differentiated between offensive and defensive weapons and included mass infantry warfare (e.g., cheap iron, allowing mass production of infantry weapons) as the offensive weapons because large mass armies could easily surpass the fortifications. He categorised chariot or cavalry warfare as defensive weapon as it requires smaller forces and can be easily stopped by fortifications and cannons as offensive weapon because it makes forts vulnerable. In short, the analysis of peace and war is mostly based on technology (Evera 1998).

Glaser and Kaufmann (1998) rejected the narrow approach of measuring offence-defence balance within the prism of military technology but included all variables like size of forces, the cumulative index of resources and nationalism. They both adopt a broad, dyadic definition of the offence-defence balance. The offence-defence impact of a specific weapon or technological invention cannot be assessed simply by considering the performance in isolation; rather, it must be evaluated by its impact on the state's ability to perform offensive and defensive missions. They argue that innovations which are primarily used by non-advancing forces lead to favourable defensive strategy while innovations which are used mainly to advance into the domain of the enemy is to be termed as offensive. Mobility, firepower, protection, logistics, communications and detection favour defence. Improvements in firepower are generally considered to favour defence as attackers are easily vulnerable to fire than defenders because they must advance, often in plain sight of defenders, making them easy to detect and to hit, whereas defenders are often well dug-in and disguised.

Lieber (2000) critically assesses the offence-defence theory to determine how technology, in particular, has shaped the relative ease of offence and defence and the probability of war. Lieber examines four technological developments since 1850 *i.e.* the emergence of railroads, the artillery and small arms revolution, the innovation of the tank, and the nuclear revolution, to challenge the conventional wisdom that certain innovations favour offence, whereas others favour defence. Lieber concludes that although technology can sporadically favour offence or defence, perceptions of a technological balance have little effect on the likelihood of war. The 'relative ease' refers to the relative costs and benefits of attacking versus defending. The terms 'offence' and 'defence' refer to actual military actions, not the political intentions, goals, or objectives that motivate military action. The theory ultimately aims to explain decisions that initiate war; the leader's expectations of war outcomes based on his/her perceptions of the strategic balance constitute a critical variable. Thus the success of any given offensive or defensive strategy is not necessarily indicative of the balance (Lieber 2000).

Tang Shipping advances a more definitive understanding of offence-defence theory. Specifically, the two critical components of the theory, *viz.* differentiation or distinguishability of weapons and military postures as either offensive or defensive, and the offence-defence balance are inadequate to explain war and peace. In the view of Shipping, weapons are simply the equipments possessed by a state's military, and nothing more. If there is a pure technological component within a state's military, it implies the nature of weaponry and nothing else. He criticised various scholars like Evera, Jones and Lieber who concentrate on an objective evaluation of balance but neither proposes an accurate definition of it (Shipping 2010). Xu Jin distinguishes between offensive and defensive military technologies. Also, military doctrines are classified into offensive and defensive strategies. A combination of technological capabilities and strategies creates a state's possible technological and strategic orientations. The four possible orientations are as follows: (a) defensive technologies and defensive strategy; (b) defensive techno land offensive strategy; (c) offensive technologies and offensive strategy; (d) offensive technologies and defensive strategy. In other words, technological development is not something that can be controlled, especially in the short term. The argument is that in periods of serious military conflict, states strive to adjust their military strategies to sustain with changes in military technology and the consequent changes that occur in the offence- defence balance. States are usually limited by their technical resources, and in the short-term, lack the consistent capacity to develop the technologies that could make their military strategy ideal. In contrast, military strategy can be transformed by will power and modification can produce substantial results in a very short period of time. Thus, during times of war or serious conflict, regulating strategy according to the existing military technology is the most practical course of action (Jin 2006).

Jack Levy examined military technology and its impact on offence-defence balance. Levy attempts a historical analysis by focusing on the measurement of the balance for the last eight centuries. The argument that the likelihood of war increases when the military technology favours the offence is theoretically possible only on the basis of the rather strong assumption that decision makers correctly perceive the offence-defence balance. Perceptions of actors do matter and constitute a critical variable; a purely objective evaluation is impossible. The balance has been defined primarily in the terms of the ease of territorial conquest, the characteristics of armaments, the resources and the incentive to strike first. Levy critiques the conception of the baseline or the zero point that indicates the transition from a defensive advantage to an offensive advantage (Levy 1984). However, there were those who argued against this line of thinking; amongst them, the most prominent is Stephen Biddle. He pointed out that only the consequences of military technology are undertaken; the balance is understudied. This is addressed by presenting and testing a systematic theory of the balance that emphasises military, strategic and tactical choices as its key determinants; this is in contrast to orthodox offence-defence theory which focuses primarily on technology. The argument is that the offence-defence balance focuses on the relative strength of the offence and defence in war which in turn depends on unit level variations in the operational concepts by which a military uses its force. The probability of a successful offensive also increases if the defender deploys its forces too shallowly or fails to maintain a mobile reserve to block any surprise breakthroughs. The ability to attack and the ability to defend are not the same and they must be differentiated. In short, Biddle argues that offensive military action succeeds when the attacker understands the method of fighting a successful breakthrough battle and the defender fails to thwart such an attack. He contends that variations in force employment are more important than technology or the size of forces in determining the outcome of military engagements (Biddle 2001).

Ted Hopf traditionally tested three elements of offence-defence balance. The first is the technical offence-defence military balance concerning the relative military advantage. He divided the offensive or defensive advantage into tactical and strategic categories. Tactical offensive advantage is the ability to seize a piece of an enemy's territory at less cost to oneself than it requires for the defender to protect it or retrieve it. A strategic offensive advantage is the ability to seize or occupy as much of an enemy's territory at less cost to oneself than is required for the defender to protect its territory or reclaim it. He also offered another element of offence-defence balance, namely, power resources which include both the available and extractable resources. The power resources constitute the material element that constitutes military and economic power. The last and the third element relates to the strategic beliefs of decision makers and the manner in which these beliefs play a role in perceiving the offence-defence balance (Hopf 1991).

Karens Ruth Adams makes an argument that prevailing technology affects the relative efficacy of offensive, defensive, and deterrent military operations and thus the incidence of attack and conquest. Specifically, attack and conquest should occur more often when technology favours offensive operations than when technology favours defensive and, especially, deterrent operations. According to him, technology implies the following: method, skills and tools that influence the ability of a state to conduct offensive, defensive and deterrent operations. He specifies the balance in terms of technologically possibility at the operational level and not in terms of the strategic, operational, or tactical moves states make (Adams 2004).

Lynn Jones responded to the various critiques on offence- defence theory. His argument is that offence-defence balance does not depend upon whether offensive and defensive weapons can be distinguished. He defined the offence- defence balance as the ease with which it can be translated into threat. It also means the amount of resources that a state must invest in offence to offset an adversary's investment in defence. He focuses on technology as it mainly determines the relative costs of offensive and defensive strategies. He also differentiates between two types of technological change which affect the offence-defence balance. First, weapons innovation may produce a new type of strategy at lower cost. Second, non-military technology innovations may reduce the costs of producing a particular type of weapon. When a technological innovation changes the relative costs of offensive and defensive capabilities, the offence- defence balance shifts (Jones 1995).

The following questions were sought to be answered in this study:

(i) To what extent does the offence-defence theory explain war and peace in International Relations?

(ii) What explains the significance of technology in offence-defence theory?

(iii)What is the impact of nuclear technology and information technology on offence-defence balance?

The research work at the outset was premised on the following hypothesis:

(i) Offence-Defence theory provides a parsimonious explanation for the outbreak of war in the international system.

(ii) The explanatory power of the offence-defence theory is determined by the balance between offence and defence, which in turn is dependent on the extent to which weaponry could be distinguished as offensive and defensive.

At the end of the study, the following inferences have been reached:

(i) Offence-Defence theory provides a parsimonious explanation for the outbreak of war and sustainability of peace in the international system. This is so because the scholars associated with the theory neglect such other variables as geographical advantage, alliance formation by the states, domestic politics within a state.

(ii) In conventional warfare the offence-defence balance fluctuates.

(iii)The defensive advantage is predominant in the nuclear context, while offensive advantage is predominant in the information warfare.

Organisation of the dissertation

The second chapter titled 'Conventional Warfare' deals with the study of offence-defence theory in the context of conventional warfare. It dwells on the role of technology in offence-defence theory. The chapter elaborates on the distinction between offensive and defensive strategies and provided ample situations in which weapons can be distinguished as offensive or defensive. The chapter examines various case studies to analyse how technological innovations shift the balance towards offence or defence. In the mid-fifteenth century, fire power and developments in heavy artillery led to a sharp resurgence of offensive superiority whereas fortifications favoured defence. During the First World War (1914-1919) the power of the offence was restored by motorised armour but on the other hand, combined effects of lethal arms like entrenchments and railroads favoured defence. During the Second World

War (1939-1945), the military doctrine and technology shifts the balance towards defence while combined armour and infantry postures amounted to offensive strategy. Technology and doctrine often combine to alter the tides of offence and defence.

The third chapter, 'Nuclear technology' analyses nuclear technology in the context of offence-defence theory. The first part of the chapter summarises the various arguments propounded by theorists of offence- defence balance. Nuclear weapons tilt the balance towards the defence on account of its inherent potential of causing mass destruction.

The fourth chapter, 'Information Warfare' examines information warfare in the arena of offensive and defensive operations. It examines the manner in which information technology could potentially affect the offence-defence balance. The chapter delves on different types of offensive warfare like 'Open Sources Intelligence' and 'Signal Intelligence' (SIGINT). The defensive warfare includes encryption, steganography, anonymity, sanitisation, trash disposal and shielding. The information warfare tends to tilt the balance towards offence as technologies and methods in offensive operation help them to attack the defensive shield thereby enabling them to acquire information resources. Thus there are difficulties in pursuing defensive operations as offensive operations are not just carried out by the individual but also by the state and non state actor. The main reason is the level of transparency in the transfer of information technologies and resources in the interconnected world. It is an offence-dominated security environment because the overall marginal cost to innovate and initiate offensive attack is very low.

The fifth chapter, 'Conclusion' sums up the major findings of the study.

Chapter Two

Conventional Warfare

Conventional Warfare

The chapter seeks to identify the role of technology in the context of conventional warfare. It will analyse the manner in which technology tends to play a vital role in shifting the balance towards offence or defence. Is technology the most critical component in determining the balance towards offence or defence in the conventional warfare era? The chapter aims to address this question precisely.

Offence Defence theory begins with a premise that it shares with the realist theory of international politics. The theory assumes that states pursue security through self-help measures in an anarchical international system. States seek to maximise their security by attempting to minimise the probability that they could be conquered or destroyed by other states. As the states exist in anarchy, they prefer to rely on their own efforts (self-help) to maximise their security. In international politics, self-help usually takes the form of unilateral acquisition of military capabilities that can be used to ensure a state's security. Although states may sometimes miscalculate or misperceive, they adopt more or less balanced policies that maximise their security. In the competitive international system, states maximise their security by using their resources efficiently. In other words, states attempt to maximise the level of security gained from the resources they invest in security (Waltz 1979).

The most common use of the concept of the offensive/defensive balance is based on territorial conquest and the defeat of enemy forces. Quester states that 'the territorial fixation then logically establishes our distinction between offence and defence' (Quester 1977: 15). On a tactical level, the offensive or defensive quality of a unit may be estimated by considering its utility in an attack upon an enemy unit like itself or in an attack upon some other concrete enemy objective, such as territory, commerce, or morale (Quester 1977).

In international politics, states have the following basic strategic options for maximising their security: defensive and offensive. States can adopt a defensive strategy that attempts to defend the territory and resources that they control and aims to make it impossible for any other state to conquer the defensive state's territory but it does not seek to expand that territory or to conquer or destroy rival states. On the other hand, offensive strategies use military conquest to expand a state's resources and potential military capabilities, to achieve a more defensive position or to conquer or threaten into submission, other states that may threaten the state. When there is an offensive advantage, an investment in offensive capabilities produces military forces that can defeat the force deployed by a state that has invested an equal amount in defensive capabilities. Under these conditions, states that want to maximise their security will invest in offence, because offensive strategies generate more security and even offensive weapons prove to be less expensive.

Technology plays a vital role in bringing about a shift in the offence-defence balance. The relative ease of attack and defence balance is determined primarily by the prevailing state of technology at any given time. Technology acts as an important determinant in balancing the ratio of offence to defence. The prospect of quick and decisive warfare exacerbates the security dilemma among states, intensifies arms race and makes war of expansion, prevention, and pre-emption more likely. When technological innovation strengthens the defence relative to the offence, states are more likely to feel secure and act benevolently. This is the most important aspect of offence-defence balance based on which the entire theory emanates (Jones 1995).

The offence-defence balance has been defined in many ways. 'The offence-defence balance is the ratio of the cost of forces that the attacker requires to take territory to the cost of the forces deployed by the defender's forces' (Glaser and Kauffman 1998: 46). The state's power multiplied by the offence-defence balance indicates its project for acquiring an effective defensive capability. When defence has an advantage, a state maintains an effective position to protect its interests with a defensive policy than an offensive one. The superior the advantage of defence, the smaller the ratio of forces required for an adequate defensive capability which in turn reduces the state's incentive to build larger forces. It also decreases the difficulty or cost of responding to its adversary's build-up. Once the state achieves an adequate defensive posture, it has incentives for restraint because continuing the build-up would suggest that the state desires an offensive capability and thus could signal ulterior motives (Glaser and Kauffman 1998).

A primary purpose of protecting territory, of course, is the protection of people and property. Defence refers to techniques and actions which is both active and passive, to deter attack, to protect people and property, to seize territory, and to minimise damage by the attacker (Tarr 1984). This linkage of territorial conquest to population defence creates a problem, however. While territorial defence was sufficient for the protection of people and property in the pre- nuclear era that is no longer true.

Hart identifies 'mobility, striking power, and protection as the essential characteristics of an offensive weapon' (Hart 1932 cited in Levy 1984: 225). Striking power is the impact of the blow which per se is not sufficient. A mobile gun contributes more to the tactical offensive than an immobile one, and its penetrating power is further enhanced if it is protected. But protection is even more important for the defence.

Studies on offence-defence theory in conventional warfare suggest that mobility favours offence, whereas firepower innovations favour defence. Almost all proponents of offence-defence theory believe that new or improved technologies that enhance mobility contribute relatively more to offence than defence. In military terms, mobility is the ability of troops and equipment to move from one place to another (Glaser and Kauffman 1998). There are essentially three types of mobility: strategic, operational and tactical.

Strategic mobility is the ability to transport military forces from the own territory to a place of operations or from one place to another. Offence defence theorists argue that greater strategic mobility allows the attacker to expeditiously transport and supply its forces far from its own borders, thus negating the defender's geographic advantage. Operational mobility is the ability to move forces within its own place. According to proponents, greater operational mobility allows the attacker to concentrate forces quickly to achieve a numerical advantage on a small portion of the front, rapidly exploit weak points in a defender's line, or oust a defender's position altogether. Tactical mobility is the ability to move forces on the battlefield. Offence-defence proponents argue that greater tactical mobility reduces the number of casualties suffered by an attacker because these losses are partly a function of the amount of time that forces are exposed to enemy in an assault (Hopf 1991). Mobility and protection are inversely related, for it is easier to protect immobile weapons and wait passively for the enemy to attack. The offensive value of the medieval knight ultimately was negated by the heavy armour which protected him but restricted his mobility (Dupuy and Eliot 1937: 103). Thus Dupuy and Eliot gave particular emphasis to the offensive advantages of mobility and striking power, noting that they too may be in conflict.

Boggs argued that mobility is the central characteristic of an offensive weapon and argues that the armament which makes possible the movement of the attacker can be said tentatively to possess relatively greater offensive power than weapons which contribute primarily to the stability of the defender (Boggs 1941 cited in Levy 1984).

Technology increases the strength of the offensive if the leader tends to adopt an offensive strategy. On the other hand it gives thrust to the defensive too. When weapons are highly vulnerable, they must be employed before they are attacked. Incentives to strike first are usually absent for naval forces that are threatened by a naval attack.

In ground warfare under some conditions, forts, trenches, and small groups of men in prepared positions can hold off large numbers of attackers. It is also argued that the offensive gained an advantage with new forms of heavy mobile artillery in the nineteenth century, but the deadlock of World War I created the impression that the defence again had an advantage. Defence would be possible even against a large and well-equipped force; states that care primarily about self-protection need not engage in arms races.

In the opinion of Jervis, the major variable that affects the security dilemma is whether weapons and policies that protect the state also provide the capability for attack. If it does not provide such capability, the basic assumption of the security dilemma remains no longer valid. A state can increase its own security without decreasing that of others. The advantage of the defence can only restructure the security dilemma. The differentiation between offence and defence may disappear. Such differentiation does not mean, however, that all security problems will be abolished. If the offence has the advantage, the probability of attack and aggression is still possible. And if the offensive advantage is great enough, status-quo powers may find it too expensive to protect themselves by defensive forces and decide to acquire offensive weapons even though this will threaten others. Furthermore, states will still have to be concerned in an important respect: that even if the other's military posture reveals a gesture of peace, it may develop aggressive intentions in the future (Jervis 1978).

Further he elaborated that the fundamental nature of defence is keeping the other side out of one's territory. A purely defensive weapon is one that can do this without being able to penetrate the enemy's land. The most obvious examples are fortifications. They can shelter attacking forces, especially when they are built right along the frontier, but they cannot occupy enemy territory. A state with only a strong line of forts, fixed guns, and a small army would not be much of a danger and can be categorised as defensive weapons. Anything else that can serve only as a barrier against attacking troops is similarly defensive. If total immobility clearly defines a system that is defensive only, limited mobility is unfortunately quite ambiguous. Short-range fighter aircraft and anti-aircraft missiles can be used to cover an attack and, unlike forts, they can advance with the troops but still, their inability to reach deep into enemy territory does make them more useful for the defence than for the offence. Any force that for various reasons fights well only in its own soil in effect lack mobility and therefore is defensive (Jervis 1978).

Weapons which are effective in reducing fortifications and barriers can be determined as offensive weapons. This is not to deny that a defensive power will want some of those weapons if the other side has them. Mobile heavy artillery is, similarly, especially useful in destroying fortifications. The defender, while requiring artillery to fight off attacking troops or to counterattack can usually use lighter guns since they do not need to penetrate such massive obstacles.

Military technology, doctrine, and force posture and deployments all affect the military offence-defence balance. Military technology can favour the aggressor or the defender. In the past, strong fortification techniques reinforced the defence, and strong methods of siege warfare strengthened the offence. Technologies that favoured mass infantry warfare (e.g., cheap iron, allowing mass production of infantry weapons) strengthened the offence because large mass armies could bypass fortifications more easily (Glaser and Kauffman 1998).

Technologies that favoured chariot or cavalry warfare strengthened the defence. In modern times, technology that gave defenders more lethal firepower (e.g., the machine gun) or greater mobility (e.g., the railroad) strengthened the defence. When these technologies were neutralised by still newer technologies (motorised armour), the offence grew stronger. Thus, when fortresses and cavalry dominated in the late middle ages, the defence held the advantage. Cannons then made fortifications vulnerable and restored the strength of the offence (Glaser and Kauffman 1998).

Technological innovations that enhance repower capability are disproportionately advantageous to the defence. First, repower allows the defender to threaten the attacker's concentration of forces before an attack. An attacker typically needs a local advantage of combat power to pierce the defender's forward defences. Numerical superiority requires density but greater density of forces provides more targets for defensive area, and thus more casualties. Second, repower favours defence because it reduces the mobility (i.e., offensive power) of the attacker. In the face of greater defensive act, an attacker must seek more armoured protection, cover, camouflage and dissemination all of which slow the attacker's advance.

Arms competition becomes a more attractive option, especially for states that enjoy a power advantage. If sufficiently large, a power advantage enables a state to achieve an effective defensive capability, in addition to an offensive capability. Although larger forces decrease the adversary's military capability, the adversary should appreciate the security pressures that make them necessary, which should reduce the political provocation they generate (Glaser 2004).

Some armaments that traditionally have been considered as defensive and therefore implicit to be 'stabilising' (in the sense that they discourage aggression and reduce the likelihood of war) are often considered to be destabilising in the nuclear age. Air defences, anti-ballistic missile defences, and even civil defences are considered under the prevailing strategic doctrine to be destabilising because by protecting populations, they threaten to undermine deterrence.

Nevertheless, even when offence has the advantage, states sometimes prefer the military status quo to an arms race for two reasons. First, although the military status quo is inadequate, a build-up could further reduce the state's security. If the state is not confident of maintaining a lead in an arms race, which is likely when states are comparably powerful, then cooperation could reduce the likelihood of still more unsatisfactory outcomes. At the same time, by agreeing not to build when it has some chance of acquiring a meaningful advantage, the state can signal its benign motives. Second, if weapons that support offensive and defensive missions can be distinguished, states have the option of pursuing qualitative arms control and limiting weapons that favour offence, while allowing those that favour defence. An agreement banning offensive weapons would enhance the state's defensive capabilities and signal benign motives (Glaser 2004).

According to Evera, when conquest is hard to achieve, states prefer to secure borders and hence are less aggressive and more willing to accept the status quo. They have less need for wider borders because their current frontiers are already defensible. They are less inclined to intervene in other states' internal affairs because hostile governments can do them less harm. On the contrary when conquest is easy, states are more expansionists because their current borders are less defensible. They desire others' geographical advantage, strategic depth, and sources of critical raw materials. They worry more when hostile regimes arise nearby because such neighbours are harder to defend against. These motives drive states to become aggressors and foreign interveners. States also resist other's expansion more fiercely when conquest is easy. Adversaries can convert smaller gains into larger conquests; hence, stronger steps to prevent gains by others are more appropriate. This attitude makes disputes more difficult (Evera 1998).

The ability to conquer others and to defend oneself is more expandable to one's control over strategic areas and resources. As a result, gains are far more for states. It can convert small conquests into larger ones and losses are less reversible. Hence, small losses can predict one's end, and small gains can open the way to hegemonic dominance. States therefore compete harder to control any assets that confer power, seeking wider spheres for themselves while fiercely resisting others efforts to expand.

This problem is compounded by its effect on state's expectations about one another's conduct. When conquest is hard, states are blessed with neighbours made benign by their own security and by the high cost of attacking others. Hence states have less reason to expect attack. This enlarges the scope of defensive policies.(Evera 1998).

Conversely, when the offence dominates, states are cursed with neighbours who are made aggressive by both temptation and fear. These neighbours see easy profits from aggression and the danger revolves around aggressive neighbours where all states face greater risk of attack. This drives them to compete still harder to control resources and create conditions that provide security. Thus states become aggressors because their neighbours are aggressors (Evera 1998).

The introduction of steam-powered railroads in the second half of the nineteenth century perhaps marked the greatest revolutionary development in military mobility. Armies were suddenly able to move and sustain huge forces across vast distances at up to ten times the speed of marching troops. The locomotives appeared in 1825, railroads spread rapidly across the European continent in the 1830s and 1840s, and by 1850, all the major powers had conducted exercises in moving and supplying troops by rail. Prussia's quick and decisive victories in the Wars of German Unification against Denmark (1864), Austria (1866), and (1870–71) have commonly been attributed to the offensive power of the Prussian railroads. In fact, railroads had much less impact on the conduct of these wars than did Prussia's superior doctrine, organisation, and material power (Jervis 1978).

The case studies related to offence-defence theory in various historical eras will show that tactical mobility is the primary criterion used to identify an advantage to the offence. In terms of the characteristics of armaments, then, tactical mobility and movement toward enemy forces and territory are the primary determinants of the offence, at least in land warfare, whereas protection and holding power contribute more to the defence. Other weapon characteristics such as striking power, rapidity of fire, and the range of a weapon systems do not contribute disproportionately to either the offence or the defence.

In the mid-15th century, fire power had moved from a secondary role to one where it was central and decisive. Developments in heavy artillery led to a sharp resumption of offensive superiority. This was symbolised by the siege of Constantinople in 1453, where the greatest of all medieval fortifications was reduced by the Turks in less than two months and proved that by the end of the 15th century, artillery had made medieval fortifications outmoded. In addition, greater mobility, and hence greater offensive capability, of this artillery is evidenced by the use of horse-drawn artillery and chains of 'wagon forts' as mobile fortifications employing bombards (Quester 1977). Small firearms also began to have a significant effect on battle at the end of the 15th century, and weakened the defence effectiveness.

Thus a drastic change in the offensive-defensive balance is said to have occurred around 1450 A.D. After 1650 A.D., the balance of military technology lay with the defence. This was largely due to the development of a new science of fortifications by Vauban and other military strategists in the late seventeenth century. These elaborate fortifications became increasingly invulnerable to artillery, and frontal assault became nearly impossible. This was the age of geometric warfare, of position and manoeuvre rather than pitched battle.

> 'Military operations were centred around fixed fortifications and were restricted by poor logistical systems and short supply lines, and guns were deficient in range, accuracy, and penetrating power' (Dupuy 1980: 144).

Frederick, the ruler emphasises on the decisiveness of the battle rather than static exercise. His willingness to take risks, his use of the oblique order as a tactical device, and his emphasis on mobility demonstrate this. In essence, Frederick differed from the norm of 18th-century warfare. The hesitancy to characterise the military balance during this period as offensive probably derives from the fact that Frederick's modernisations were primarily tactical and strategic rather than technological (Levy 1984).

The period between 1815-1856 witnessed a blend of arms and diplomacy which favoured defenders. Mass armies disappeared, British economic power grew, and Britain acted as a balancer on the continent. Continental powers expected Britain to balance and believed British strength could not be overridden. This defence-dominant arrangement lasted until mid-century. It began weakening before the Crimean War (1853-56). When war in Crimea broke out, military factors still favoured defenders, but leaders underestimated the power of the defence. Britain and France launched their 1854 Crimean offensive in false anticipation of quick and easy victory but in general, diplomatic factors favoured the defence (Evera 1998).

As the Crimean War was defensive, in the post-Crimean War, the offence-defence balance shifted further towards the offence. Mass armies favoured the offence, but as small arms and railroads expanded, the offence tilted the balance towards the defence. In the diplomatic realm, however, the power of defenders fell dramatically because defence-enhancing diplomacy largely broke down. Most important, Britain entered an isolationist phase that lasted in the 1870's, and Russia lost interest in maintaining the balance among the western powers. As a result, diplomatic obstacles to continental conquest largely disappeared, giving continental aggressors a fairly open field. This diplomatic change gave France and Sardinia, and then Prussia, an offensive opportunity, which they exploited by launching a series of wars of opportunistic expansion in 1859, 1864, 1866, and 1870.

In 1859, British and Russian neutrality gave France and Sardinia undue advantage, which they used to seize Lombardy from Austria. In 1864, British, Russian, and French neutrality gave Prussia and Austria opportunity, which they used to grab Schleswig-Holstein from Denmark. In 1866, British, French, and Russian neutrality gave Prussia full authority against Austria, which Prussia used to smash Austria and consolidate its control of North Germany. In 1870, Bismarck guaranteed the neutrality of the other European powers by shifting responsibility for the war to France and convincing Europe that the war stemmed from French expansionism. As a result, Prussia again had a free hand to fulfil its expansionist aims. It used this to shatter France, confiscate Alsace-Lorraine, and secure control over South Germany (Evera 1998).

In the period (1871-90), the defence dominated because of Bismarck's new diplomacy and Britain's replenished activism. In diplomacy, Bismarck embarked on defensive alliances that deterred aggressors and calmed status quo powers after 1879. British power diminished slightly, but this was offset by the recovery of Britain's will to play the balancer (Evera 1998). By mid-century, or by 1870 at the latest, the balance had shifted in favour of the defence, which continued through World War I. This is due to the holding power of entrenchments, barbed wire, the machine gun, the breech-loading rifle, the difficulty of frontal assault and closing with the enemy, and to the generally static nature of warfare as demonstrated in the American Civil War, the Russo-Turkish and Russo-Japanese Wars, and others.

In 1898, Germany launched a naval build-up that was intended to challenge the British navy, which was significantly amplified four times in the years before World War I. In the consequent arms race, Germany failed to undermine Britain's naval capabilities. Britain interpreted the build-up as a signal of malign intention. German motives, which combined with the increase in German naval forces, led Britain to increase cooperation with Russia and France. Germany's sense of encirclement contributed to its growing insecurity, making war more likely. The question is whether this bad outcome reflected Germany's goals and the international conditions it faced, or instead suboptimal policies. This is a case of power disadvantage and defence advantage that left Germany unable to acquire the capabilities, it desired. Although Germany's naval policy was intended to challenge the political status quo and elevated Germany to a world power, its naval strategy was militarily defensive. To achieve success on the defence, Germany judged that there is a need to be two-thirds the size of the British fleet attempting to impose a close blockade. In other words, when opposing a British blockade, defence had the advantage, and this 3:2 ratio worked to Germany's advantage (Glaser 2004).

With the beginning of the American Civil War and extending through World War I, there was a trend toward enormous increase in the masses of men under arms, and in the range, casualty-producing capacity, and rapidity of fire of infantry weapons, without any counteracting growth in the means of advancing of this fire. This conclusion reinforces the view that the balance favoured the defence in 1914. The interwar period presents a similar gap between the analysis of military historians and the perceptions of statesmen (Boggs 1941 cited in Levy 1984).

The First World War (1914-1919) showed mixed result, but overall the offence increased by 1939. The combined effects of lethal small arms (accurate fast-firing rifles and machine guns), barbed wire, entrenchments, and railroads gave the defence, an enormous advantage during the First World War. The first three – lethal small arms, barbed wire, and trenches gave defenders, a large advantage at any point of attack. The fourth, railroads, let defenders reinforce points of attack faster than invaders could, because invaders could not use the defenders' railroads given that railroad gauges differed across states, and defenders destroyed rail lines as they retreated while the defenders had full use of their own lines (Jervis 1978). Technology and doctrine combined to define these tides of offence and defence. Sometimes technology overrode doctrine, as in 1914-18 and in 1945- 91 (when the superpower militaries embraced offensive doctrines but could not find offensive counters to the nuclear revolution).

During the Second World War, doctrine shaped technology, when blitzkrieg doctrine fashioned armour technology into an offensive instrument. States shape the military offence-defence balance by their military posture and force deployments. Thus, Stalin eased attack for both himself and Hitler during 1939-41 by moving most of the Red Army out of strong defensive positions on the Stalin Line and forward into newly seized territories in Poland, Bessarabia, Finland, and the Baltic states. This left Soviet forces better located to attack Germany and far easier for Germany to attack, as the early success of Hitler's 1941 invasion revealed. The US eased offence for both itself and Japan in 1941 when it deployed its fleet forward to Pearl Harbour and bombers forward to the Philippines.

The German leaders believed the offence as even stronger than what it was. Military doctrine and technology gave the defence the advantage until the late 1930s, when German blitzkrieg doctrine combined armour and infantry in an effective offensive combination. This offensive innovation was unrecognised outside Germany and doubted by many in Germany, but Adolf Hitler, firmly believed in it. This reflected his faith in the offence as a general principle which is imbibed from international social Darwinist propaganda in his youth (Bell 1986).

In 1930 or so, the military technology favoured the offence. The speed, mobility, and striking power of the armoured division with tactical air support had a great advantage to take over field defences and minor fortifications. The new warfare was characterised by fluidity and speed, deep penetrations, and broad encirclements. The stalemate of World War I had been transformed into the blitzkrieg of the World War. Most observers at the time, however, perceived that the military technology favoured the defence (Quester 1977).

More importantly, the workings of interwar diplomacy unbolted a wide political opportunity for Nazi expansion. Britain fell into a deep isolationism that left it less willing to commit its declining power to restrain continental invaders. The United States also withdrew into isolation, and removed the counterbalance that checked Germany in 1918. Austria-Hungary would have balanced against German expansion, but its smaller successor states leaned to bandwagoning. This let Hitler to enlarge German influence into southeast Europe by coercion and subversion. The Soviet Union and the Western powers failed to cooperate against Hitler (Bell 1986).

Britain also feared that a defensive alliance against Hitler would arouse German fears of allied encirclement, spurring German aggressiveness. This chilled British enthusiasm for an Anglo- French-Soviet alliance. Hitler overstated the already-large advantage that diplomacy gave the offence because he thought bandwagoning overcomes balancing in international affairs. This false faith shaded all his political forecasts and led him to vastly miscalculate other states. Before the war he failed to forecast that Britain and France would balance German power by coming to Poland's rescue. Once the war began, he believed Germany could threaten Britain into seeking alliance with Germany after Germany crushed France, or he later held, after Germany ruined the Soviet Union. He thought the United States could be scared into staying neutral by the 1940 German-Japanese alliance. In short, Hitler's false theories of diplomacy made three of his most dangerous opponents shrink to insignificance in his mind (Bell 1986).

Hitler thought his conquests would arouse little countervailing opposition from distant neutral powers. As a result, he believed that he faced opportunity for aggression. Unlike 1914, the late 1930s were not a pure case of perceived offence dominance. Instead, the 1930s saw status quo powers' perceptions of defence dominance create real offensive opportunities for an aggressor state. Hitler thought the offence to be strong and even exaggerated its strength, but other powers (the Soviet Union, Britain, and France) underestimated its strength. Their perceptions of defence dominance relaxed their urge to jump the gun at early signs of threat (as Russia did in 1914). This made things safer but this perception also relaxed their will to balance Germany, because they found German expansion less frightening.

The propositions all suggest is that there is something about military technology itself that affects the likelihood or nature of war. This relative advantage may be one of 'the several variables affecting the likelihood of war by affecting policy, but itself is analytically distinct from policy' (Levy 1984). The offensive-defensive balance of military technology is defined primarily in terms of the ease of territorial conquest, the nature of armaments, the resources needed by the offence in order to overcome the defence, and the incentive to strike first (Levy 1984).

It is evident from the above-mentioned analysis that the offence-defence theory is shaped by the technology that is available to states. At any given time, the existing pool of technology determines the relative costs of offensive and defensive strategies. Two types of technological changes affect the offence-defence theory. First, weapons innovation may produce a new type of strategy at lower cost. The development of cannons and other siege machinery, for example reduced the cost of launching offensive strikes against fortified castles. Without such weapons, offensive against castles required long sieges or infantry assault across moats and battlements. Second, non-military technological innovations may reduce the costs of producing a particular type of weapon.

The development of the tank shifted the offence-defence balance in favour of the offence. If this is true, reductions in the unit costs of tanks will produce a larger offensive advantage. In practice, the offence-defence theory can be assessed by asking whether existing technology makes it relatively easy for a state to use an offensive strategy to conquer another state of roughly equal strength. When a technological innovation changes the relative costs of offensive and defensive capabilities, the offence-defence balance tends to shift. The offence-defence balance is a continuum and the direction of such shifts is more important than whether the balance simply favours the offence or the defence (Levy 1984).

Offence-Defence theory does explain the idea that the individual types of weapons can be classified as either entirely defensive or entirely offensive. But it should also be taken in the consideration that the theory properly argues that at any given time, the set of existing and available military technologies determines the relative costs in terms of offensive and defensive security strategies. Recall that the offence-defence balance is defined in terms of the amount of resources than a state must invest in offence or (defence) to offset an adversary's investment in defence or (offence). It is the weapon technology that plays a critical role in determining the relative cost of offensive and defensive strategies. Individual weapons system almost invariably combines technologies that can be labelled offensive or defensive. The net result according to offence-defence theory is that states can deploy invulnerable retaliatory forces at relatively low cost making conquest virtually impossible.

Offence-Defence theory continues to shape contemporary foreign policy debates on arms control, conventional and nuclear deterrence and force posture, the prevention of civil and ethnic conflict, and the so-called revolution in military affairs. The most policy relevant conclusion offered by offence-defence theory is that arms race, conflict and war may be prevented through carefully designed arms control agreements that either deliberately shift the balance of technology toward defence or seek to correct misperceptions of the balance.

Offence-Defence Theory in conventional warfare tends to shift the balance either towards offence or towards defence. The historical overview of different epochs shows the manner in which inventions of several technologies affect the balance. The developments of innovative technologies in different periods of time virtually impacts upon the trend of offence-defence theory.

Chapter Three

Nuclear Technology

Nuclear Technology

The chapter analyses offence-defence theory in the context of the emergence of nuclear weapons in the post-Second World War era. The first part of the chapter dwells on various strands of opinion within offence-defence theory. According to offence-defence theorists, the shift tilted to defence as the repercussion of nuclear war led to mass destruction of life and property in the Second World War. The usage of nuclear weapons and its devastating effects constrain the countries to indulge in war.

Concerning nuclear weapons, it is generally agreed that the balance tilts towards the defence. Attack makes no sense, not because it can be beaten off, but because the attacker will be destroyed in turn. In terms of the questions under consideration here, the result is the equivalent to the primacy of the defence.

First, security is relatively cheap. Less than one percent of the Gross National Product (GNP) is allocated to deterring a direct attack on the state. Most of it is spent on acquiring superfluous systems to provide a lot of insurance against the worst feasible possibilities. Second, both sides can simultaneously gain security in the form of second-strike capability. Third, second-strike capability can be maintained in the face of wide variations in the other side's military posture. There is no purely military reason as to why each side has to react quickly and strongly to the other's increases in arms. Any kind of spending that the other devotes to trying to achieve first-strike capability can be neutralised by the state's spending much smaller sums on protecting its second-strike capability. Fourth, there are no motivations to strike first in a crisis. Important problems remain, of course. Both sides have interests that go well beyond the defence of the homeland. The protection of these interests creates conflicts even if neither side longs expansion. Furthermore, the shift from defence to deterrence has greatly increased the importance and perceptions of solution. Defence now rests on each side's conviction that the other would prefer to run high risks of total destruction rather than sacrifice its vital interests (Jervis 1978).

The states that could take their population out of hostage, either by active or passive alter the status quo. The desire to prevent such a situation was one of the rationales for the anti-ABM agreements. It explains why some arms controllers opposed building ABM's to protect cities, but favoured sites that covered ICBM fields. Similarly, many analysts want to limit warhead accuracy and favour multiple re-entry vehicles (MRV's), but oppose multiple independently targetable re-entry vehicles (MIRV's). The former are more useful than single warheads for penetrating city defences, and ensure that the state has a second-strike capability (Jervis 1978).

Stephen Evera explains that after 1945, two changes manipulate the offence-defence balance back toward the defence. First, the end of American isolationism transformed European political dealings. The United States replaced Britain as continental balancer, bringing far more power to bear in Europe than Britain ever had. As a result, Europe in the years after 1945 was unusually defence dominant from a diplomatic standpoint. Second, the nuclear weapons provided defenders, a large military advantage so large that conquest among great powers became practically impossible. Conquest now required a nuclear first-strike capability (the capacity to launch a nuclear strike that leaves the defender unable to inflict undesirable damage in retaliation). Defenders could secure themselves merely by maintaining a second-strike capability (the capacity to impose unacceptable damage on the attacker's society after absorbing an all-out strike). The characteristics of nuclear weapons – their immense power, small size, light weight, and low cost ensured that a first-strike capability would be very hard to attain, while a second-strike capability could be sustained at little cost. As a result, the great powers became effectively unattainable, and even lesser powers could now stand against far stronger enemies.

Overall, the nuclear revolution gave defenders an even more asymmetrical advantage than the machine gun-barbed wire-entrenchments-railroad complex that emerged before 1914. American and Soviet Union policymakers grabbed this vast military revolution only slowly. At first many alarmed that nuclear weapons would be a boon to aggressors but this fear proved wrong. The vast advantage that it gave defenders was only vaguely recognised and it is partly because leaders failed to explain it. As a result, state behaviour changed only slowly, and both superpowers competed far harder - in both Central Europe and the third world than objective situations required. The Cold War was far more peaceful than the preceding forty years, but could have been still more peaceful if Soviet Union and US leaders would have understand that their security problems had immeasurably weakened (Evera 1998).

There are two reasons to distinguish between defence and deterrence dominance. First, defensive and deterrent operations are distinct. As Glenn Snyder explains, deterrence discourages the enemy from taking military action by painting a prospect of cost and risk that overshadows his/her probable growth. Defence means reducing our own prospective costs and risks in the event that deterrence fails. Deterrent operations involve punishment; defensive ones, damage restraint. Second, attack and conquest should occur more often in defence-dominant eras than in deterrence-dominant ones. It is so because, in the absence of the survivable and deliverable weapons such as nuclear weapons that makes deterrence dominant by dramatically increasing the costs of miscalculation states face fewer costs for playing the chances. Moreover, in defence-dominant eras, states face incentives to prepare for future revolutions in military affairs by extending their perimeters to make it hard for other states to conquer them (Snyder 1961).

Jack Levy too analysed the shift towards the defence. With the invention of atomic bomb in 1945, deterrent operations became far easier and more vigorous than ever before. Nuclear weapons greatly increase the costs which states might have to pay for attacking others' territory and vital interests, thereby making deterrent operations dominant Since 1946, the small size of nuclear weapons and advances in transportation and missile technologies have meant that nuclear weapons can be easily delivered to their targets, whether by bomber, land- or sea-based missile, ship, truck, or even airline passenger. The surplus of options makes deterrence dominant (Levy 1984).

According to offence-defence proponents, when all sides in a conflict possess a secure second-strike nuclear capability, *i.e.,* when no side can launch an attack that is successful enough to prevent retaliation from the other, the defender has an enormous advantage over the attacker. This conclusion is counter-intuitive and requires clarification because under conditions of mutual assured destruction (MAD), no side can defend against a nuclear attack. Offence-defence theory codes nuclear weapons as defence dominant because it is relatively easier and less costly for states to maintain a retaliatory capability than to build a force capable of taking away another's retaliatory capability (Glaser and Kaufmann 1998).

The exceptionality of the nuclear age lies in the fact that the defeat of the adversary's military forces and territorial infiltration is no longer necessary for the destruction of his/her population centres. The destruction of population and the coercive power that it makes possible are no longer conditional upon military victory. For this reason, the protection of territory from invasion is analytically distinct from the protection of population. The likelihood of war presumably increases as territorial conquest becomes easier, because the probability of victory increases while its expected costs decrease. But the ability to destroy enemy population and industrial centres contributes to deterrence in the nuclear age, and therefore it decreases the likelihood of war or at least nuclear war (Schelling 1966).

Although it is in the nuclear age that deterrence has been elevated to a high position, the concept itself is an old one and goes back to the very beginnings of human conflict. In its most simple form, deterrence is a specific type of relationship in which an actor, a state, group or an individual- seeks to influence the behaviour of another in desired directions. While a party can influence another in many different ways, deterrence is distinctive. Under deterrence, an actor A seeks to prevent another B from undertaking a course of action which A considers undesirable, by threatening to impose unacceptable costs upon B in the event if the action is taken (Mohan 1986).

Before examining the nature of nuclear deterrence, it must be pertinent to review the two types of deterrence that existed in the pre-nuclear era. One is the passive deterrence, which seeks to dissuade an adversary from initiating war. Passive deterrence is an attempt to convince the opponent that he/she cannot be successful and denying him/her the objectives and goals he/she seeks. The second type, active deterrence, consists of readiness and capability to inflict unacceptable punishment and pain, in the event of deterrence failing.

In the nuclear realm, the focus is on comparisons of the attacker's value for territory to the costs that the attacker would incur as a result of nuclear retaliation against its society. During the Cold War, an assured destruction capability was the standard most commonly used in gauging the adequacy of US forces. Given this standard, taking territory at an acceptable cost of fighting translates into the ability to eliminate the defender's assured destruction capability. The offence-defence balance would be the ratio of the cost of forces required to undermine the defender's assured destruction capability to the cost of the defender's forces. If we chose a lower level of retaliatory damage as our standard, the attacker's forces would have to be more effective, shifting the offence-defence balance further toward defence advantage (Glaser 1992).

Thus nuclear weapons favour the defender by greatly improving the ability to deter by punishment. States are deterred from attacking one another in a nuclear world; and deterrence is the functional equivalent of defence. The theory basically aims to explain when states feel secure and when they do not or, alternatively, when they can deter attacks and when they cannot. When states rely on deterrence for their security, forces that augment deterrence are essentially defensive. In a world of conventional arms, deterrence becomes easier as the defender is increasingly capable of denying territorial gains to the attacker. In the nuclear world, deterrence rests on the defender's ability to punish the attacker with unacceptable costs for attempted aggression. The only way to seize territory at a tolerable cost in the nuclear world is by eliminating the defender's second-strike capability. This is very difficult to do, however, because it is much easier to enhance one's own deterrent forces than to strengthen forces that threaten the foe's deterrent forces (Snyder 1961).

The consequences of nuclear warfare in a Mutually Assured Destruction (MAD) world are easy to follow and tremendously difficult to undo. Large and extreme shifts in the offence-defence balance that have occurred with the nuclear revolution have had a significant effect on international politics. The most fundamental prediction of offence-defence theory is that war among nuclear powers would not occur.

If the no-war prediction is taken consideration, the prospect of devastation in a nuclear conflict is enough to deter even the most highly expansionist country. The robust security provided by nuclear weapons almost eliminates fears that might lead status quo states to launch defensive or pre-emptive wars. In short, the improbability of obtaining military victory, not to mention a quick and decisive one makes war among the nuclear powers virtually obsolete. Second, according to offence-defence theory, arms racing should not occur once states believe they have acquired the capability for assured nuclear retaliation. This prediction has both a quantitative and qualitative element.

In quantitative terms, adversaries will be little concerned with comparing the relative size of their nuclear arsenals because even large shifts in relative force levels pose little threat to the 'weaker' side's ability to retaliate and inflict unacceptable damage. The qualitative aspect of the no-arms-race prediction is that once states find themselves in a MAD world, they should not attempt to gain an advantage at the nuclear level by building offensive counter force weapons, which are aimed at destroying an adversary's strategic nuclear weapons. Possession of an assured destruction capability already provides states with a high degree of security. A first-strike advantage is virtually unfeasible and impossible to maintain, and thus unreasonable to follow. A final prediction that offence-defence theory makes about behaviour under nuclear defence dominance is that states should not compete or fight too intensely over territory beyond their own territory or the territory of close allies (Lieber 2000).

In the Cold War, offence-defence theory envisages minimal intervention and competition between the superpowers and the third world countries. Nuclear weapons make conquest much harder, and vastly enhance the self-defence capabilities of the superpowers. It allowed the superpowers to take a more relaxed attitude toward events in the third world, since it now requires much more catastrophic events to shake their defensive capabilities. Whatever had been the strategic importance of the third world in a non-nuclear world, nuclear weapons have vastly reduced it (Lieber 2000).

Specifically Waltz explains that proliferation will lead to a decrease in the level of interstate violence because nuclear weapons anyhow, deter threat or retaliate posing unacceptable damage (Sagan and Waltz 2003). The opposing argument questions the very logic of deterrence as suggested above when it comes to nuclear weapons. Aron for example, argues that new proliferators may not be as rational as the original nuclear states. Thus, as nuclear weapons spread, the deterrence that operated between the Soviet Union and the United States of America during the Cold War might not apply (Aron 1965).

Drawing from Waltz and the rational deterrence literature, we can argue that states facing the possibility of a nuclear attack will be more willing to concede or back down from violent conflict. The proliferation optimists contend that nuclear weapons raise the stakes so high that states are unlikely to go to war when nuclear weapons enter the equation. The pessimists challenged that new proliferators are not necessarily rational and that having nuclear weapons does not discourage war but rather makes war more dangerous. On the other hand, optimists contend that actors will show more restraint in crises involving more participants with nuclear weapons. Waltz suggests thus: 'weapons and strategies change the situation of states in ways that make them more or less secure' (Sagan and Waltz 2003: 6).

As Waltz argues, the higher, the stakes and the closer a country moves toward winning them, the more sure that the country invites retaliation and risks its own destruction. States are not likely to run major risks for minor gains. War between nuclear states may rise as the loser uses larger and larger warheads fearing that, states will want to draw back. It is not the escalation but de-escalation which becomes possible. War remains possible, but victory in war is too dangerous to fight for (Sagan and Waltz 2003). 'Nuclear war simply makes the risks of war much higher and shrinks the chance that a country will go to war' (Snyder and Diesing 1977: 450).

Using similar logic, Bueno de Mesquita and Riker demonstrate formally that a world with almost universal membership in the nuclear club is less likely to experience nuclear war than a world with only a few members (Bueno de Mesquita and Riker 1982). Feaver argues that 'even a modest nuclear arsenal should have some existential deterrent effect on regional enemies, precisely because decapitation is so difficult' (Feaver 1992- 93: 186). There are those who argue that security is increased at a systemic level when the number of nuclear states increases; the level of uncertainty created is high when more than one or two players are playing with a nuclear deck.

If this happens, 'the probability of deliberate nuclear attack falls to near zero with three, four, or more nuclear nations' (Brito and Intriligator 1983: 137). Cimbala agrees, arguing that 'it is only necessary to threaten the plausible loss of social value commensurate with the potential gains of an attacker' (Cimbala 1993: 194). The causal mechanism in a proliferation optimist argument like that of Waltz (Sagan and Waltz 2003), which expects war to be less likely as the number of nuclear states increases is connected to a rationalist view of nuclear deterrence Proliferation optimists implicitly contend that, as the number of nuclear actors in the system increases, the amount of disputes involving nuclear actors should increase as well. That is, all else being equal, the more of any type of actor you add to the playing field of international politics, the more likely that that type of actor will be involved in a crisis. If nuclear weapons increase the prospects of deterrence, then proliferation should result in more crises with constrained actors that are prone to back down instead of escalate (Sagan and Waltz 2003).

Rational deterrence proceeds on the notion that actors are effectively able to deter other states from aggression if they have credibly positioned themselves as determined and strong states. States with nuclear weapons should be especially effective at deterrence if they can convince their adversary that there is some possibility that nuclear weapons would be used against them (Huth 1999). Nuclear states may choose brinkmanship or costly signals to overcome the credibility problem. There is some probability that if a state would use a nuclear weapon against an opponent, the scale of the costs of that event should be enough to deter opponents from escalating in a conflict even if the probability of that event is low (Schelling 1962).

Nuclear deterrence is a function of both capabilities and credibility. The capability to inflict great damage is the only necessary condition for deterrence, and the strength of deterrence will generally be improved as the credibility of nuclear use increases. The logic is probabilistic in that nuclear weapons should at least decrease the likelihood of violent conflict but not eliminate it. The formal models of Zagare and Kilgour suggest that as an actor increasingly values the status quo more than fighting, the ability for deterrence to succeed increases. If it is functional to nuclear weapons and if a state making a demand faces higher expected costs of war because of the threat of nuclear retaliation, then that actor is more likely to prefer backing down to fighting.

Under this logic, the nuclear state might raise its demands until the other actor has a reasonable relative valuation of fighting and the probability of war is roughly the same as if there were no nuclear deterrent. However, if demands are made according to a risk-return-trade-off, under similar assumptions modelled by Powell, then increases in the expected costs of war of an opponent should be greater than any increases in the demands of exploitive actors. So, the probability of war should decrease as the costs of war increase, even if the demands also increase in response. The invention of intercontinental missiles and nuclear warheads has brought into question, conventional concepts about the nature of war, the uses of military force in the pursuit of national policy, and the role of military power in the maintenance of international stability (Powell 1999).

Stability as defined is the absence of war and major crises. The concept of stability is larger and more complex than simply the presence or absence of war. As noted by Patrick A. Mc Carthy, it is overly simplistic and more than erroneous to label a changing system unstable or to label an unchanging system stable (Mc Carthy quoted in Hussain 2005). Bernand Loo argues that strategic stability must be linked with geography to help create a more nuanced idea of strategic stability. He defines strategic stability as a condition where policy makers do not feel pressurised into making reactive changes from existing non violent to violent strategies involving the large scale use of military force in the pursuit of particular state interests. The concept of strategic stability does not rule out the use of military force. What it does rule out is accidental or unintentional war as well as immediate reactions of policy makers who feel that they are being pushed or pulled almost against their will towards decisions about the use of military force without prior consideration of other non violent policy options (Loo 2003).

Therefore, it is more important to discuss stability in the nuclear context. Deterrence stability comprises elements like the absence of incentives for rapid qualitative or quantitative expansion of a state's nuclear arsenal *vis-a vis* that of an adversary and the effectiveness of deterrence in reducing incentives for major coercive political changes in behaviour induced by the threat of the use of force. Nuclear deterrence is thus as much a product of politics as it is that of perceptions and technology.

Deterrence stability is also crucial to preventing war between nuclear adversaries.

> A balance of deterrence a situation in which the incentives on both sides to initiate war are outweighed by the disincentives is stable when it is reasonably secure against shocks, alarms and perturbations. That is it is stable when political events internal or external to the countries involved, technological change accidents false norms misunderstandings, crises limited wars or changes in the intelligence available to both sides are unlikely to disturb the incentives sufficiently to make deterrence fail (Schelling and Halperin 1962).

Deterrence stability on the other hand also explains that each side is convincingly deterred (in relation to threats to core norms, values and interests) by the other and thus deterrence rests on the following: (a) means to deter; (b) ability to carry out deterrence threats; (c) willingness to carry out deterrent threat; (d) assured control of deterrent forces; (e) rational adversary making expected cost-benefit analysis (Gregory 2005).

This chapter further examines the implications of possession of nuclear weapons for relations between India and Pakistan. It will analyse how offence-defence theory explains the relations between the two countries. The main ground to prefer this as a case study is that the states are *de facto* nuclear weapon states. Historically, they are antagonistic to each other right from their independence in 1947. They had waged full fledged conventional war three times – 1947, 1965 and at last 1971. After the conduct of nuclear tests in 1998, we could witness no major war between the two countries. It will examine whether nuclear weapons deter both the countries from waging war and whether the balance shifts towards defence.

The decision to conduct nuclear test was a momentous one for India. The tests of May 1998 were overwhelmingly popular with the public at large, but the decision emerged over decades, with much opposition along the way. Even today, Indians who view nuclear deterrence as a difficult and demanding task believe that India will be unable to develop and deploy a nuclear force sufficient for the deterrence of China. In their view, the main effect of India's developing nuclear capabilities was to cause Pakistan to develop its own. India is therefore worse off with nuclear weapons than it would have been without them.

The stability and instability of nuclear deterrence between India and Pakistan also has been a major issue of concern since the late 1980's. Proponents of nuclear deterrence in South Asia, who argue that the introduction of nuclear weapons has prevented the outbreak of a large-scale conflict between India and Pakistan, generally belong to the "state-as-a- rational-actor" school of thought.

The past behaviour of India and Pakistan shows that there is little or no danger of either side firing a nuclear weapon in anger or because of miscalculation. In all three wars, both sides avoided wars of attrition or deliberate targeting of population and industrial centres. The leaders in both capitals insist that nuclear weapons are only for deterrence and are not weapons of war. History shows that nuclear weapons are usable only against an opponent that does not have the ability to retaliate in kind such as the United States against Japan in 1945. The only exception to this rule might be the case of a state that faced total imminent destruction. It is conceivable that Pakistan could use nuclear weapons if faced with total defeat by India. Indians argue, however, that they have no interest in destroying the Pakistani state and incorporating another 140 million Muslims into the Indian state (Malik 2003).

Despite the 1999 Kargil War and the post-11 September 2001 brinkmanship, both of which illustrate the 'stability-instability' paradox that nuclear weapons have introduced to the equation in South Asia, (Lavoy 1995), proponents of nuclear deterrence in India and Pakistan believe that nuclear deterrence is working to prevent war in the region. They point to the fact that neither the 1999 Kargil conflict nor the post-11 September 2001 military standoff escalated beyond a limited conventional engagement due to the threat of nuclear war. So the stability argument is based on the reasonable conclusion that nuclear weapons have served an important purpose in the sense that India and Pakistan have not gone to an all-out war since 1971. Just as nuclear deterrence maintained stability between the United States and the USSR during the Cold War, so it can induce similar stabilising effects in South Asia. Regarding the technical requirements of stable deterrence, questions about command, control, and safety procedures continue to be raised. Both Pakistan and India claim to have maintained tighter controls over their arsenal. It is not in their own interests to see non-state actors gaining control of nuclear technology. Both India and Pakistan publicly have declared moratoriums on further nuclear tests, and India's adherence to

No-First-Use (NFU) posture and confidence-building measures such as pre-notification of missile tests and an agreement not to attack each other's nuclear installations promotes crisis stability (Malik 2003).

Post-11 September 2001, procedures to promote greater security and control over nuclear weapons and materials have been accorded the topmost priority. India's nuclear arsenal is firmly under the control of civilian leadership, and the Pakistani army always has preserved the real authority over its country's nuclear weapons, regardless of who is the head of state. Pakistan's military chain of command appears undamaged despite internal turmoil and reshuffling at the top of the government. The United States reportedly is considering the prospect of offering assistance to ensure the physical protection of sensitive nuclear assets with sensors, alarms, meddle proof seals and labels, and other means of protection, ensuring personnel uniformity and secure transport of sensitive items (Malik 2003).

In short, Indian and Pakistani policymakers and strategic analysts see nuclear weapons as essential to maintaining state security and ensuring state survival. From their perspective, nuclear deterrence prevents conventional wars, keeps peace, and brings warring parties to the negotiating table - the Lahore (1999) and Agra (2001) summits are good examples.

Deterrence depends on the ability of both sides, particularly the politically defensive one, to keep it credible, by demonstrating both military capacity and political resolve with the threat to go to war. The military capacity built and maintained over time, must be capable of inflicting such pain and destruction on the enemy as to dissociate him/her from incentives for surprise or pre-emptive attack (either out of confidence or in desperation). When the defensive power is inferior or even equal to the offensive power, it requires at minimum, strategic forces diversified at relatively large weapon inventories and capable of certain and entirely destructive retribution. The attacker must know that his survival as a possible state would be put in peril by his surprise or pre-emptive attack (Zoppo 1966).

The late Pakistani chief of the army staff, General Mirza Aslam Beg, remarked that 'India and Pakistan can no longer fight even a conventional war over Kashmir, and his counterpart, the chief of the Indian army staff,' General Krishnaswami Sundarji, concurred: 'Kargil showed once again that deterrence does not firmly protect disputed areas but does limit the extent of the violence'. Raja Menon put the larger point simply: 'The Kargil crisis demonstrated that the sub continental nuclear threshold probably lies territorially in the heartland of both countries, and not on the Kashmir cease-fire line. The obvious conclusion to draw from Kargil is that the presence of nuclear weapons prevented escalation from major clash to full-scale war. This contrasts harshly with the bloody 1965 war, in which both parties were armed only with conventional weapons (Menon 2000).

Sagan points out that the survival of Indian and Pakistani forces cannot be guaranteed but it can neither guarantee their complete destruction, and this is what matters. Conventional weapons put a premium on striking first to gain the initial advantage and set the course of the war. Nuclear weapons eliminate this premium. The initial benefit is irrelevant if the cost of gaining it is half a dozen cities. More important than the size of arsenals, the sophistication of command and control, the proximity of competitors, and the history of their relations, is the sensibilities of leaders. Fortunately, nuclear weapons make leaders behave sensibly even though under other circumstances, they might be hasty and careless. Sagan believes that future Indian-Pakistani crises may be nuclear. Once countries have nuclear weapons, any confrontation that merits the term 'crisis' is defined as a nuclear one. With conventional weapons, crises tend toward instability because of the perceived, or misperceived, advantage of striking first. Nuclear weapons make crises stable, which is an important reason for believing that India and Pakistan are better off with than without them. Yet because nuclear weapons limit escalation, they may tempt countries to fight small wars (Sagan and Waltz 2003).

Ashley Tellis has argued that India-Pakistan deterrence is more stable than it is given credit for: The prospects for deterrence stability are high because no South Asian state is in a position to secure any political objectives through the medium of major conventional and by implication of nuclear war. This condition is only reinforced by the high levels of defence dominance obtaining at the military level and thus it is not at all an overstatement to say that deterrence stability in South Asia originates simply from the inability of India and Pakistani to successfully prosecute quick and decisive conventional military actions especially with respect to wars of unrestricted aims. This makes the situation stable and this is the fact that neither India nor Pakistan has the strategic capabilities to implement those successful damage limiting first strikes that might justify commencing nuclear attacks in a crisis (Tellis 2001).

The main reason for the decisive influence of nuclear weapons in the context of international stability is the awesome destructive potential of nuclear war and the unbelievably compressed time in which such destruction could take place. Moreover, no country wherever located and however strong militarily can, under current and foreseeable circumstances, realistically believe itself immune from the power and reach of nuclear weapons. Nuclear weapons and their delivery mechanisms are manifestations of an unprecedented and spectacular intrusion of technology into politics.

Deterrence has received a great deal of scrutiny in South Asia but there is little agreement about whether it operates and if so how. It could be concluded that even if nuclear weapons are dangerous for mankind and could lead to incredible devastation, it acted as a tool in preventing a major war between the countries and provided stability in the international system. After its invention, there is no further third world war. The leaders have understood the credibility as well the capability of nuclear weapons. It is used as defensive weapon as the state neither attacks nor pokes another country to become offensive.

Chapter Four

Information Warfare

Information Warfare

This study seeks to analyse the politics of Information Warfare in the arena of offensive and defensive operations. It will investigate how the information warfare affects the balance in offensive and defensive operations. It will validate the role of information warfare in shifting the balance either towards offence or defence. In the first part, the chapter aims to examine the fundamental concepts needed to understand the broad spectrum of activities encompassed by the Information Warfare phenomenon. It provides a theoretical background to these activities, and examines the context in which these are most effective. Further it analyses the role of offensive and defensive technologies in the field of information warfare and seeks to understand as to how the interplay of offensive and defensive technologies operates in information warfare.

By definition, the fundamental weapon and target in information warfare is 'information'. It is the product that has to be manipulated to the advantage of those trying to influence events. The means of achieving this are manifold. Protagonists can attempt to directly alter data or to deprive competitors of access to it. Using other, more subtle techniques, the way the data is interpreted can be changed by altering the context that it is viewed. Thus, a range of activities is manifest in information warfare.

> Information Warfare consists of those 'actions intended to protect, exploit, corrupt, deny or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an advisory'(Denning 1999: 10).

Martin Libicki, has proposed seven categories of Information Warfare theory that identify specific type of operations: (a) command and control warfare – attack on command and control systems to separate command from forces;(b) intelligence based warfare – the collection, exploitation and protection of information by systems to support attacks in other warfare forms; (c) electronic warfare – communications combat in the realms of the physical transfer of information (radio electronic) and the abstract forms of information (cryptographic); (d) psychological warfare - combat against the human mind; (e) hacker warfare - combat at all levels over the global information infrastructure; (f) electronic information warfare - control of economies via control of information by blockade or imperialistic controls;(g) cyber warfare-futuristic abstract forms of terrorism fully simulated combat, and reality control (Libicki 1995).

> "Information war is a product of the information age which to a great extent utilizes information technology and information ordnance in battle. It constitutes a networkisation of the battlefield, and a new model for a complete contest of time and space" (Pufeng 1995: 37).

The origins of the term 'information warfare' can be traced back to the late 1980's when the expression was specific to the military domain. It became a known concept in the Gulf War of 1991. The origins of information warfare are electronic warfare, military deception, psychological operations and information/operational security. However, the most significant element in its evolution was the development of electronic computing and communications technology. By the 1990's, the role of this technology in warfare had been proven in the 1991 Gulf War (Campen 1992).

In the new post-Cold War period, information warfare has taken its place in the era of national security. Recently, the increasing use of technology and its significance in today's society has revolutionised the communication process as well as the implications of what Information Warfare necessitates. Information Warfare has found its roots in the mid-twentieth century when technology advanced during World War II. The historical background of Information Warfare could be traced with the encryption device used in Germany in World War II called the Enigma machine. It was used to encipher messages to troops; the Allies were able to defeat the Germans by deciphering the Enigma code by way of offensive measures of information warfare. This proved to be very beneficial to the Allied victory in World. War II. Furthermore, the Gulf War in the early 1990's marked a crucial moment in the use of IW as a key to its victory on the front lines. Military and commercial use of satellite communications, navigations, surveillances and intelligences gave advantages to the United States of America and its allies over Iraqi forces. Hence, the lack of defensive measures of information warfare proved to be a key factor in defeating the Iraqis (Horvath 2001).

Information or more specifically, information technology had given the edge in battlefield intelligence, targeting, and command and control. By the mid-1990's, information warfare, driven by considerable developments in computer and communications technology, was developing into an integrated doctrine but still it was technology which was focused with command and control dominating, and with media management still as a separate entity. However, technological innovations were beginning to see them merge. It was becoming clear that modern wars were also media wars. Nevertheless, information warfare was still predominantly military in nature and it was assumed to only be relevant to a wartime context (Libicki 1995).

Alvin and Heidi Toffler (1993) approach the history of warfare using a model of three waves. The following sections briefly discuss these three waves:

Agrarian wave

The agricultural revolution started the first great wave of change in the history. It led to the first of today's known societies. Agriculture enables communities to produce economic products which in that age were the cause of many wars. The link between war and soil was close at this time. The people were kept ignorant by their statesman to keep them focused on farming and warfare.

Industrial wave

The industrial revolution changed the way wars were fought. The element of mass production introduced weapons of mass destruction (nuclear and chemical). The mass armies were not loyal to the landowners but to modern nation states which were paying the soldiers. The change from one wave to the other did not happen in a short period but, similar to the industry, took its time to change the warfare.

Information wave

In the late 1970s and early 1980s, third wave technologies and ideas began to change the industrial wave societies. The mass society became slowly a communication society. With this development, the military doctrine began to change. The duality between the two waves was expressed in the Gulf War of 1990-91 where a dual war was fought by the allies. On one hand, mass destruction was used like in World War II with large bomb carpets over the enemy troops but on the other hand, high tech weapons were used to aim the targets precisely (Toffler and Toffler 1993).

Technological changes brought out several implications for information operation such as economic availability, technological ownership and information access. The easy accessibility of information technology to individuals reduces the economic advantage that powerful governments have traditionally held over other states, terrorist groups or even individuals. The availability of these technologies to small forces probably enables them to contact offensive attacks in the information domain, though offensive action in the physical domain would be improbable due to asymmetry in conventional military force capability. The lack of an identifiable enemy together with economic recession, has contributed to lack of consensus among states and international organisations on the nature and scope of global security. While the need to address the proliferation of weapons of mass destruction persists, the scope of security issue in the post-cold war era increasingly includes issues such as new kind of warfare and operations other than war (Waltz 1998).

These following are some examples of available (or possible) information warfare weapons:

Computer Viruses

A virus is a code fragment that copies itself into a larger program, modifying that programme. A virus executes only when its host programme begins to run. The virus then replicates itself, infecting other programmes as it reproduces. Viruses are well known in every computer based environment, so that it is not astonishing that this type of rough programme is used in the Information Warfare. It could imagine that the Central Intelligence Agency (CIA) (or Army, Air Force) inserts computer viruses into the switching networks of the enemy's phone system. As today's telephone systems are switched by computers, it can shut them down, or at least causing massive failure, with a virus as easy that it can shut down a "normal" computer. An example what the damage a virus could cause exists (Greenberg 1998).

Worms

A worm is an independent programme. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programmes. Also if worms do not destroy data like the

Internet Worm, they can cause the loss of communication with only eating up resources and spreading through the networks. A worm can also easily be modified so that data deletion or worse occurs. With "wildlife" like this, one could imagine breaking down a networked environment like ATM and banking network (Greenberg 1998).

Trojan Horses

A Trojan horse is a code fragment that hides inside a programme and performs a disguised function. It's a popular mechanism for disguising a virus or a worm. A Trojan horse could be disguised as a security related tool for example like SATAN (Security Administrating Tool for Analysing Networks). SATAN checks UNIX system for security holes and is freely available on the Internet. If someone edits this program so that it sends discovered security holes in an e-mail message back to him (lets also include the password file? No problem), the Cracker learns much information about vulnerable hosts and servers. A clever written Trojan horse does not leave traces of its presence and because it does not cause detectable damage, it is hard to detect (Greenberg 1998).

Information technology is disseminating into virtually all military weapons, communications, and command and control systems, as well as the civilian systems that support modern industrial (or post-industrial) economies and their military efforts. As such, information warfare includes both new techniques, such as computer infringement and interruption and telecommunications spoofing, and old ones, such as scam, obscure and physical attacks on observation posts and lines of communication. The use of such tools as computer intrusion and computer viruses, for example, may take war out of the physical, kinetic world and bring it into an intangible, electronic one.

These newer forms of attacks are the products of science fiction and range along continuums extending from those with no physical impact on the enemy to some that would cause grave destruction or loss of life. These have no physical invasion beyond national borders to those requiring traditional, military invasions, and from those affecting purely civilian targets to those hitting purely military ones. Attacks could be conducted from a distance, through radio waves or international communications networks, with no physical intrusion beyond enemy borders. Damage could arise from military or civilian deaths or from system breakdown, to the denial of service of important military or governmental systems during the time of crisis. It can cause widespread fear, economic hardship, or merely cause inconvenient for civilian populations to access their information systems in their daily lives.

The compliance about Information Warfare (IW) is that it is used by states that are acquainted with high technologies. Information War on the battlefield will therefore be used mostly by them. Unfortunately, today, most potential enemies do not have the technological capability which make them easily vulnerable and that is the reason why IW can successfully be used against them. The enemy has to have high tech weapons and communication to use IW in a practical manner which is apparently not feasible.

The Information Warfare weapons could more likely be used in the near future as terrorist weapons rather than on the battlefield by the regular armies. Today's communication society is extremely vulnerable to disruptions. Instead of planting a bomb in an airplane with all the dangers for the terrorists, they could shut down all the communication capabilities from the tower of an airport to the hundreds of airplanes that the control centre guides. An accident following this disruption would be most likely (Haeni 1997).

> The offence/defence balance of military technology has been defined primarily in terms of the ease of territorial conquest, the characteristics of armaments, the resources needed by the offence in order to overcome the defence and the incentive to strike first' (Levy 1984:22).

Offensive and Defensive capabilities are mainly centred on the security planning. Offence seeks to use force to gain control over assets or compel loss of control; defence seeks to use force to retain control over assets and limit damage. Once conflict is commenced, victory is ultimately determined by superior technology, ability, and execution that either overcomes the defensive measures or blunts the offensive thrusts (Adams 2003-04).

The main focus of the offence-defence framework is the offence-defence balance (ODB) as an explanatory variable. Most of the hypotheses found in this literature suggest specific dynamics can be associated with strategic environments that bias towards offence, towards defence, or are balanced. Studies have found, for example, that an offence favourable balance leads to a higher incidence of war; certain forms of alliances; more intense arms racing; brinksmanship and crisis escalation; and, higher barriers for international cooperation with the opposite dynamics holding true when defence dominates (Biddle 2001: 745).

It must be argued that an offence-defence strategic framework must be adopted, once again, in order to think about and organise against threats in cyberspace. The dominant technology of the day and the manner in which it can be effectively employed structures the strategic military environment and dictates the approach that must dominate.

Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information. Information-based processes are information systems, and computer-based networks while protecting one's own actions which are designed to achieve advantages over military or business contender (Goldberg 1993).

Information Warfare consists of both offensive and defensive operations. Offensive operations are aimed at targeting and exploiting information resources, the objective is to shift the balance in favour of the offensive player. The gain to the offensive player may take several forms. It could incur financial loss, when information resources are stolen or bank records are altered or it could also be military or political advantage. The gain represents the value of the operation to the offensive player, the outcome of which depends on the resources, the player and the operation itself. Similarly the loss to the offensive player may take several forms. It could be financial losses from the theft of property or loss in productive owing to computer resources being unavailable and the workers being idle. It could be lost power, political support or bargaining position. Thus, like the gain, the loss is a function of resources, and also stimulates nature of operation (Denning 1999).

Offensive information warfare operations produce a win-lose outcome by altering the availability and reliability of information resources to the benefit of the offence and disadvantage of the defence. There are three general outcomes. First, the offence acquires greater access to the information resource. This was illustrated by the Iraqi acquisition of intelligence documents from the German spy and the allied acquisition documents from the German spy and the allied acquisition of information about the battle space from spy satellites. Second the defence loses all or partial access to the resource; that is, the resource becomes less available to the defence. This was illustrated by the attacks that sabotaged Iraq's command and control and radar systems and by Saddam's censoring of broadcast media. Third, the integrity of the resource is diminished. This was illustrated by the TV broadcasts that aired misleading or distorted stories such as amphibious exercise (Denning 1999).

Many operations produce multiple effects. Acts of disruption such as those against Iraq's command and control systems both deny access and damage integrity. Computer intrusion give the hacker greater access to computer systems while diminishing the integrity of the system, especially if files are altered. Some operations begin with an acquisition phase and then move on to sabotage or use a combination of both throughout. Therefore offensive technologies are manual weapons requiring human planning, testing and delivery. Enabling technologies will improve the understanding of weapon effect on large scale network, facilitating the introduction of semi automated control to conducted structured attacks on networks. Integrated tools will stimulate, plan and conducted these semi automated attack. Emerging technologies will expand the complexity of attacks to provide large scale network control with synchronized perception management of large population.

Defensive Information Warfare on the other hand aims to protect information resources from three form of attack: increased availability to the offence, decreasing availability to the defence or decreased integrity. The goal is a cost effective defence, the cost of safeguard should be less than the losses that would occur in their absence. There are different types of defences like prevention, deterrence, indication and warning, detection, emergency preparedness and response. The defensive mechanisms are not mutually exclusive and some mechanisms fall into more than one category.

Defensive information warfare is closely related to information security. They are not however indistinguishable. Information security is concerned mainly with owned resource and with protecting against error, accidents and natural disaster as well as intentional acts. Defensive information warfare addresses non owned resources including broadcast and print media in the public domain, but is not concerned with unintentional acts.

Information security is widely accepted as a benchmark of defending the state from the emerging threat of Information Warfare. The state has role in defensive information warfare and information assurance relating to its broad responsibilities in the area of national security, economic security, public safety, law and order and general well-being of nation. However, offensive operations are carried not only by individuals or private group but also by the state itself in war and intelligence operation. The technologies and method in offensive operation help them to attack the defensive shield thereby enabling them to acquire information resources.

Thus there are difficulties in pursuing defensive operation as offensive operations are not just carried out by individuals but also by the state and non state actors, the reason being that there is transparency in the transfer of information technologies and resources in the interconnected world. It is likely that the availability of information recourses is exploited for the purpose of gathering intelligence. However, the increasing availability of this formation has the potential to minimise uncertainty amongst states.

The terms Open Sources Intelligence '(OSINT)' refers to intelligence operation that uses information gained from unclassified sources. It includes requirements analysis, information filtering and analysis and integration of information after it has been collected. It was conducted to answer a specific question in support of some mission. 'Competitive intelligence' refers to the corporate use of open sources intelligence against business competitors, for example, to determine as much as possible about business plans. Although the acquisition of information from open sources is not necessarily an act of information warfare, it becomes information warfare when the person or organisation affiliated with the information loses from the acquisition and would not have agreed to it. The collector thus gains value from the information at the expense of the party. Sensitive information can be acquired directly from open source, or it may be inferred from non-sensitive material, for example, by aggregating material drawn from multiple sources.

Open source intelligence is by far the dominant mode of intelligence gathering, even within the US Department of Defence. It can be cheap, fast, and timely. Except when it infringes privacy or intellectual property rights, it is generally legal. Its limitation is that it may not uncover critical information that is accessible only with the spies and surveillance (Denning 1999).

Intelligence agencies use the term 'signal intelligence (SIGINT)' to refer to the broad range of operation that involves the interruption and analysis of signals across the electromagnetic spectrum. After interception, the signals are decoded, decrypted, translated, summarised and analysed to produce and intelligence product. SIGINT is also conducted by law enforcement agencies in criminal investigations and certain businesses use SIGINT to monitor their employees. SIGINT encompasses communication intelligence (COMINT) and electronic intelligence (ELINT), which includes the use of radar. These forms of intelligence are generally converging in terms of digital processing techniques used and shared use of the spectrum in the radio-radar-range.

Defensive Technologies that are now being deployed by both military and commercial domain provide layers of security to bridge the gap between the two approaches. The first generation and military 'trusted' computers are based on the formal analysis or testing with strong cryptography. Second, commercial technologies – computer, UNIX or Windows Operation Systems and networks – with components like firewalls, software wrapper, smart card authentification etc helps to manage risk and achieve a specified danger of security for operation over the non secure Global Information Infrastructure (GII) .

Technologies of defensive operations perform functions like encryption, steganography, anonymity, sanitisation, trash disposal and shielding. Cryptography does for electronic information what locks do for printed information. Information is protected by scrambling with a secret key. The scrambled information called 'ciphertext' is totally unknown to anyone who does not know the key. The process of producing the ciphertext is called encipherment or encryption, the reverse process restoring the original message called 'plaintext' is called decipherment or decryption. Encryption system or cipher is built from two basic types of transformation: transformation and substitutions. Transpositions (permutations) re-arrange bits or characters, whereas substitutions replace bits, characters, or blocks thereof with substitutes. These transformations are keyed so that a single method can be used with different results. Confidentiality encryption is a process of encoding an electronic communication so that only the orignater and receiver of the particular message will able to read it (United Nation 2002). To decrypt, one must know both the method and the key under which it was encrypted. While the key is kept secret, the method itself is often made public so that it can be shared by many people and implemented in hardware and software products.

Steganography is the method of hiding a message in such a manner that its very existence is concealed. This is done by imbedding the message in some medium such as document, image, sound recording, or video. Anyone who knows the medium that contains a secret could promptly extract the massage, assuming that method of encoding is known. The purpose of using steganography is different for different groups in society. The use of steganography by terrorists or non-state actors underlines the ambiguity that governments feel over the cheap, readily available, powerful encryption tools that are now in widespread use due to globalisation of information technologies. Civil libertarians see the use of strong ciphers as right of citizen in a free state and believe that access by government to the encrypted communication of its citizens could be disastrous if an authoritarian regime came to power. Government agencies, on the other hand, fear that criminals such as terrorists, drug runners and gangsters will use encrypted communication to carry on their activities without interference from the law (Goebel 2007)

Shielding is another way of concealing information. In the physical environment, secret facilities can be hidden under a layer of camouflage. Stealth aircraft, spy satellites and weapon can be coated with anti-radar-detection shielding to foil radar detector. Public pay phones and Automated Teller Machine (ATM) machine can use shielding to help keep shoulder surfers from picking up phone and back card numbers as they are keyed in.

The overall marginal cost to innovate and initiate offensive attack is considerably low. The technology (hardware/software) is widely available and continues to become more accessible (ease of use and financial cost). For example, in an attack against financial institutions in 2009 off- the-shelf software available for $40 was modified to penetrate the ATM systems of the Royal Bank of Scotland. Second, the skills needed to use digital technology and computer-based networked systems are proliferating across the global population exponentially as there are more computer-literate teenagers than nuclear physicists. The combination of accessible technology and growing skill sets creates a lively innovation environment. When put into military security terms, while nothing prohibit innovation on defensive measures, there is very little burden toward innovation itself and; therefore, it can be assume that a foundational feature of the strategic cyber environment is constant offensive innovation. Cyber attackers expend little of their offensive potential in probes and exploration (and even broader, low level attacks) relative to defensive countermeasures they face, and, therefore, are not deterred by the prospect of attacks that fail to achieve success (Gates 2009). As the balance shifts towards offence it could be determined as information warfare as an offence-dominated security environment.

It is an environment of offence dominance in which deterrence is easily overwhelmed. Therefore, anchoring national security around the goal of avoiding war is a recipe for defeat. When it comes to cyber, this means that the states must set aside deterrence as the overarching concept. This raises the challenge of applying in one area of threat management (cyber) a different framework than is to be applied elsewhere (Freedman 2004).

Stephen Biddle suggested that the combination of the base technology, the numerical balance of forces and the core tactics available to combatants will define the offence-defence strategic balance. A preliminary application of these traditional military measures to cyberspace supports the assessment of an offence-dominant environment. Not only does the technology have a significant marginal cost advantage, but the reservoir of offensive forces can be organised to gain numerical advantages that are exponentially greater than what is available to the defence (Biddle 2001).

This is a structural condition of cyberspace. It is already noted on the offensive side, the ability to bring tens of thousands of computers together as botnet armies, but it is important to note the rather fragmented nature of defensive forces. Critically, defensive forces are divided across the broad private-public gulf. For example, government agencies charged with protecting US critical infrastructure are limited in their ability to actively participate in the defence of those infrastructures that are privately-held and privately defended.

Within specific private industry, there is a structural obstacle to coordinated defence in that each company is an economic competitor of each other. There are limits to the coordination possible between one bank and another bank due to proprietary rights. In fact, 'competing' for customers by being better at securing one from identity theft is built into the business model. While better coordination between government and industry and across private companies can develop to work against disastrous failures, a level of fragmentation will remain and, thus, create an offensive advantage and defensive disadvantage.

Perhaps most significantly, the operational opportunities open in cyberspace again bias toward the offence. Biddle notes that to the level to which cover, concealment, dispersal of forces, mobility, and rapid infliction of cost are available to offensive forces, the ODB will favour the offence. In information warfare, all of these measures are in place. Cyber aggressors can cover their attacks with ease and concealment (avoiding attribution) remains high. Attacks can come from many edges simultaneously using servers and digital devices globally. The mobility gained from being able to move attacks from one server base to another line of attack again shifts the advantage towards the offence. Finally, the sheer speed of cyber aggression creates an enormous advantage. The 2009 Federal Bureau of Investigation (FBI) indictment in the Royal Bank of Scotland case notes that over $9 million dollars was stolen from 280 ATMs worldwide in a matter of hours. Again, structural limitations on the defensive side compound this advantage on the offensive side (Biddle 2001).

Defence in depth requires more burdensome programming, intrusive management of systems, and coordination across private-public networks. None of which is likely to be easier to sustain than offensive innovations. Across all measures, cyberspace is an extreme case of an offence-dominated environment. Deterrence is unachievable in such a battle space (Harknett et.al 2010)

Ease-of-access is one of the main advantages of the digital world and an inherent feature of the internet and related digital technologies. If concerned about security-defence, one naturally assumes a primary organising principle of limiting access; the internet and related technologies are built on the opposite default principle. The convenience and efficiency gained through easy access are now essential cornerstones of life in the digital world. The system and its structure cannot be reinvented, but only modified. Thus, more code can be 'layered' into networks, but this cannot close the offensive advantage. More defensive code, counter-intuitively, may in fact produce more opportunities for offensive operations. Overburdened systems will tend to crash more easily and more sophisticated security protocols may be ignored by users requiring more automation, or in the language of an offence-defence environment, more catastrophic breakthrough points.

Most communication signals are vulnerable to interception, some can be with little effort but others requires sophisticated tools and considerable resources, because the nature of the attack is passive as opposed to active attacks which deny or distort the signals. Interception tools include microphone receivers, tape recorders, telephone taping devices, cellular scanners, radio receivers, spy satellite, computer network sniffers and filters for isolating the information of interest. Parabolic microphones can detect conversations over a kilometer away and laser versions can pick up conversations behind a closed window in the line of sight (Denning 1999).

Offensive information warfare through offensive technologies takes advantage of weakness in defensive technologies. States embrace military secrets confidentially when the offence is dominant. This causes rational over arming, as states measure their defence efforts to worst case estimates of enemy strength, on a ground that under spending is disastrous and overspending is wasteful (Evera 2000)

A major weakness in the failure of defensive technologies in containing information warfare is the lack of security awareness and training programmes to the operators.

Security awareness and training programmers can serve to inform employees about information security policy of concerned organisation. The idea is to protect them from risk and potential losses and train them in the use of security practices and technologies. However, training in these technologies is mostly confined to technological dominant countries.

According to Joyner and Lotrointe, the large extent of advanced military technologies and the new ways in which they affect states are labelled 'Information Operations' and these within IW is considered a subset. These Information Operations provide logisticians with the ability to know what weapons are in their inventories and where to focus attention, as well as the information necessary to know where a target is, its defences and how to destroy it. The growing weapons of Information Warfare are expanding, like a 'logic bomb' or a 'computer worm' (Joyner and Lotrointe 2001)

The above discussion makes the argument that states are vulnerable to attack and the balance tilts towards offence. Information Warfare probably constructs the situation when defence is unaware of the danger and accidentally is more prone to offensive operations. Cyber aggression exists in a realm of constant attack and counteraction. It is a strategic environment of offence-defence that requires a national cyber security strategy. This emphasises the need for war-fighting capabilities, rather than war avoidance postures. Improved security will rest on the country obtaining defensive capabilities that can actively blunt attacks (as opposed to dissuade them) and offensive capabilities that can advance state interests and mitigate the damage of enemy attacks by degrading their capacity to sustain such attacks.

Chapter Five

Conclusion

Conclusion

The purpose of the study is to examine the explanatory power of offence-defence theory. It was an attempt to understand the factors that influence the offence-defence balance. The role of technology in determining the balance has been explored.

The interplay of offence and defence is a theme which focuses on warfare. Offence produces war and empire; defence supports independence and brings about peace. The offence-defence theory contends that international conflict and war are more likely when offence has the advantage, while peace and cooperation are more feasible when defence has the advantage. The offence-defence balance is shaped by the technology that is available to states. The broader definition of the offence-defence balance conflates variables of different types. Technology, in principle, is more or less acquired by all the states in a given international system and therefore is a general variable. Geographical conditions and the cumulative index of resources, on the other hand, vary from state to state. Therefore, the major focus of research concentrates on technology and not at the situational factors that shape the security and strategy of states.

Offence-Defence theory posits that at any given time the set of existing and available military technologies determines the relative costs of offensive and defensive security strategies. When there is an offensive advantage, it means that available technologies make it less expensive for states to seek security by adopting offensive military posture and strategy.

An investment in offensive capability produces a military force that can defeat the force deployed by a state that has invested an equal amount in defensive capabilities. Under these conditions, states that want to maximise their security will invest in offence; offensive strategies generate more security. Moreover, offensive capabilities are less expensive than defensive ones. When defence has the advantage, it means that available technologies ensure that defensive military postures and strategies will yield more security per investment.

Individual weapons systems at the given circumstances can be labelled as offensive or defensive. The pool of available technologies at any given time determines the cost of building weapons and deploying military capabilities that can be used in support of an offensive or defensive strategy. The offence-defence balance can be assessed by asking whether existing technology makes it relatively easy for a state to use an offensive strategy to conquer another state of roughly equal strength. A technological innovation could change the relative cost of offensive and defensive capabilities thereby shifting the offence-defence balance.

The offence-defence theory predicts that international politics will become more competitive and less peaceful when the offence-defence balance shifts towards the offence. It explains that in a world where there is an offensive advantage, expansionist grand strategies will be more common, states will adopt offensive military doctrines and arms race will emerge. In general, war will become more probable. The greater the offensive advantage, the more severe, these consequences will be. For example, in conventional warfare, technologies that favoured mass infantry warfare (e.g., cheap iron, allowing mass production of infantry weapons) strengthened the offence because large mass armies could bypass fortifications more easily.

Mobility, striking power, and protection are essential characteristics of an offensive weapon. The combined effects of lethal small arms (accurate fast-firing rifles and machine guns), barbed wire, entrenchments, and railroads gave the defence, an enormous advantage during World War I. The first three – lethal small arms, barbed wire, and trenches – gave defenders a large advantage at any point of attack. Developments in heavy artillery led to a sharp revival of offensive superiority. The entire period could not be declared only as offensive or defensive; the reason is that at any given point of time, a set of technologies determines the cost of offensive or defensive strategies.

Nuclear weapons revolutionised the custom of war in the twentieth century. Before the production of such weapons in 1945, states in conflict could weigh their chances of military success against an adversary based on expected costs and benefits of going to war. Since the introduction of nuclear weapons, however, the balance of this strategic calculus has changed considerably. Nuclear weapons are characterised by such high destructive capacity that it imposes such a heavy price on states; they deter states from becoming offensive and shifts the balance towards defence.

In nuclear age when nuclear weapons surpass the conventional weapons the balance no longer fluctuates between offence and defence. Nuclear revolution has significantly shifted the offence-defence balance towards defence. A state that attempts to attack another state that possesses nuclear weapon is likely to be destroyed itself. This deters the states to attack and shifts the balance towards defence. In this age too, technology plays a major role in determining the offence-defence balance. Nuclear deterrence makes it possible for relatively weak states to prevent much stronger states from conquering them. History shows that nuclear weapons are usable only against an opponent that does not have the ability to retaliate in kind such as the United States against Japan in 1945.

Information warfare represents the so-called information revolution led by the ongoing rapid evolution of cyberspace, microcomputers, and associated information technologies. The concept of information warfare began as a technology oriented tactic to gain information dominance by superior command and control. This soon developed into a realisation of the power of information as both a 'weapon' as well as a 'target'. The technology determines the balance and in information technology, the balance tilts towards the offence. The ambiguity of attacks in information warfare stems from the fact that the originating sources are hard to trace. However, the attacks are useful in terms of deception. For example, an information warfare attack on Indian defence computer system could be made to appear as if it originated from a Pakistani source even if it really came from a hacker in Argentina.

The information technology is distinguished as offensive advantage as the states are more or less unaware of the attack. The information warfare would swiftly wipe away all the information related to security and makes the attacked states more vulnerable towards the attacker. Therefore, the impact of information technology on the offence-defence balance is simple: it signifies the victory of offence. Offensive advantage is predominant in the information warfare.

Since the late 1970's, when it emerged, offence-defence theory continues to dominate Security Studies and International Relations. This study demonstrates that the theory provides a parsimonious explanation for the outbreak of war and sustainability of peace in international system. The initial hypotheses that were proposed at the beginning of the study are therefore validated. In conventional warfare the offence-defence balance fluctuates. The defensive advantage is predominant in the nuclear context, while offensive advantage is predominant in the information warfare. However, the explanation pertaining to war and peace offered by the theory revolves within the ambit of technology. Technology tends to play a major role in determining the balance in offence-defence theory. An accurate assessment of the the offensive or defensive advantage of a given technology in a given situation would probably enhance the predictive power of the theory.

References

References

(* indicates a primary source)

Adams, Ruth Karen (2003-04), "Attack and Conquer: International Anarchy and the Offense-Defense Deterrence Balance," *International Security*, 28 (3): 45-83.

Aron, Raymond (1965), *The Great Debate Theories of Nuclear Strategy,* Translated by Ernst Pawel, New Jersey: Double Day.

Asal, Victor and Kyle Beardsley (2007), "Proliferation and International Crisis Behaviour", *Journal of Peace Research,* 44 (2): 139-155.

Biddle, Stephen (2001), "Rebuilding the Foundations of Offense-Defense Theory," *The Journal of Politics*, 63 (3): 741-744.

Bell, P.M.H. (1986), *The Origin of the Second World War in Europe*, London: Longman.

Boggs, M. W. (1941), "Attempts to Define and Limit 'Aggressive' Armament in Diplomacy and Strategy", *University of Missouri Studies,* 16 (1): 44-54.

Brito, J.L. and M.D. Intriligato (1996), "Proliferation and the Probability of War: A Cardinality Theorem", *Journal of Conflict Resolution,* 40 (1): 206–214.

Campen, A.D. (1992), *The First Information War: The Story Of Communications, Computers, And Intelligence Systems in the Persian Gulf War,* Fairfax, VA: AFCEA International Press.

Cimbala, J.S. (1998), *The Past and Future of Nuclear Deterrence*, Westport, CT: Praeger Publishers.

Denning, Dorothy E. (1999), *Information Warfare and Security*, Singapore: Addison Wesley Longman.

Dupuy, T.N. (1980), *The Evolution of Weapons and Warfare*, Bloomington: Indiana University Press.

Dupuy, R.E. and G.F. Eilot (1937), *If War Comes,* New York: MacMillan.

Evera, Stephen Van (1999), *Causes of War, Volume 1: The Structure of Power and the Roots of War,* Ithaca N.Y.: Cornell University Press.

-------------------------, (1998), "Offence, Defence and the Causes of War", *International Security*, 22 (4): 5-43.

Feaver, P. (1992/93), "Command and Control in Emerging Nuclear Nations", *International Security,* 17 (3): 160-187.

Freedman, Lawrence (2004), *Deterrence,* Malden, MA: Polity Press.

Glaser, Charles L. and Chaim Kaufmnann (1998), "What Is Offence-Defence Balance and Can We Measure It?", *International Security*, 22 (4): 44-82.

Glaser, Charles L. (1992), "The Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models", *World Politics,* 44 (4): 497-538.

-------------------, (2004), "When Are Arms Races Dangerous? Rational versus Suboptimal Arming", *International Security*, 28 (4): 44–84

Gates, Robert (2009), "Cyber Attack A Constant Threat.". [Online: web] Accessed 21 April, 2011 URL: http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml.

Goebel, Greg (2007), "Frontiers in Cryptography", [Online: web] Accessed 29 June, 2011, URL: URL: http://www.Vectorsite.net/ttcode_12html.

Goldberg, Dr. Ivan. "1993 Institute for the Advanced Study of Information Warfare" [Online: web] Accessed 1 1April 2011, URL: http://www.psycom.net/iwar.1.html.

Gray, Colin S. (1993), *Weapons Don't Make War: Politics, Strategy, and Military Technology,* Lawrence: University Press of Kansas.

Greenberg, T. Lawrence et al. (1998), *Information Warfare and International Law*, Washington D C: National Defense University Press.

Gregory, S. (2005), "Rethinking Strategic Stability in South Asia," [Online: web] Accessed 30 June 2011, URL: http://www.sassi.uk.com/pdfs/shaungregory_RR3.pdf.

Joyner, C and Lotrointe C. (2001), "Information warfare as International Coercion: Elements of a Legal Framework", *European Journal of International Law*, 12 (5): 825-866.

Haeni, E. Reto (1997), *Information Warfare: An Introduction*, Washington DC: The George Washington University.

Harknett, J. Richard et al. (2010), "Leaving Deterrence Behind: War-Fighting and National Cyber security," *Journal of Homeland Security and Emergency Management*, (1): 1-26.

Hart, B. H. L. (1932), "Aggression and the Problem of Weapons", *English Review*, 55: 71-78.

Hopf, Ted (1991), "Polarity, the Offence Defence Balance and War", *American Political Science Review,* 85 (2): 475-49.

Horvath, Eric (2001), "Information Warfare: The Unconventional Art in a Digital

World. Sans Institute", [Online: web] Accessed 30 June 2011 URL: http://rr.sans.org/infowar/infowar.php.

Hussain, R.S. (2005), "Analysing Strategic Stability in South Asia with Pathways and Prescriptions for Avoiding Nuclear War ", *Contemporary South East Asia*, 14 (2): 141-153.

Huth, P.K. and B. Russett (1990), "Testing Deterrence Theory: Rigor Makes a Difference', *World Politics,* 42 (4): 466-501.

Jervis, Robert (1979), "Deterrence Theory", *World Politics*, 31 (2): 289-324.

----------------- (1978), "Cooperation under the Security Dilemma", *World Politics*, 30 (2): 167-214.

Jin, Xu (2006), "The Strategic Implications of Changes in Military Technology", *Chinese Journal of International Politics*, 1 (2): 163–193.

Jones, Lynn M Sean. (1995), "Offence-Defence Theory and Its Critics", *Security Studies*, 4 (4): 660-691.

--------------- (2000), "Does Offence-Defence Theory Have a Future?" [Online: web] accessed on 18 November 2010 URL:http://www.ciaonet.org/wps/lys03/lys03.pdf

Lavoy, P. (1995) "The Strategic Consequences of Nuclear Proliferation", *Security Studies*, 4 (4): 739-40.

Levy, Jack S. (1984), "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis", *International Studies Quarterly*, 28 (2): 219-238.

Lieber, Keir A (2000), "Grasping the Technological Peace: The Offence-Defence Balance and International Security", *International Security,* 25 (1): 71-104.

Libicki, Martin C. (1995), *What is Information Warfare?*, Washington DC: National Defence University.

Loo, B. (2003), "Geography and Strategic Stability", *The Journal of Strategic Studies,* 26 (1): 157-174.

Menon, R. (2000), *A Nuclear Strategy for India,* New Delhi: Sage Publications.

Mesquita, de Bueno Bruce and W. Riker (1982), "An Assessment of the Merits of Selective Nuclear Proliferation", *Journal of Conflict Resolution* 25(2): 283–306.

Malik, Mohan (2003), "The Stability of Nuclear Deterrence in South Asia: The Clash between State and Anti State Actors", *Asian Affairs* 30 (3): 177-199.

Mohan, Raja C. (1986), "The Tragedy of Nuclear Deterrence", *Social Scientist*, 14 (4): 3-19.

Pufeng, Wang (1995), *Information Warfare and the Revolution in Military Affairs* Beijing., Junshi Kexueyuan.

Powell, R. (1999), *In the Shadow of Power,* Princeton, NJ: Princeton University Press.

Quester, George H (1977), *Offence and Defence in the International System,* New York: John Wiley and Sons.

Sagan, S.D and Kenneth Waltz (2003), *The Spread of Nuclear Weapons: A Debate Renewed with New Sections on India and Pakistan, Terrorism and Missile Defense,* New York: W.W Norton & Company

Schelling, C.T. and M.H. Halperin (1962), *Strategy and Arms Control*, New York: Twentieth Century Fund.

Schelling, C.T. (1962), "Nuclear Strategy in Europe", *World Politics*, 14 (3): 421-433.

------------------ (1966), *Arms and Influence*, New Haven: Yale University Press.

Shiping, Tang (2010), "Offence-Defence Theory: Towards a Definitive Understanding", *The Chinese Journal of International Politics*, 3 (2): 213-260.

Snyder, G.H. (1961), *Deterrence and Defense: Toward a Theory of National Security*, Princeton: Princeton University Press.

Snyder, G.H. and P. Diesing (1977), *Conflict Among Nations*, Princeton, NJ: Princeton University Press.

Snyder, Jack L. (1984), *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914,* Ithaca: Cornell University Press.

Tarr, D. (1984), "Defense as Strategy: A Conceptual Analysis", in S.J. Cimbala (ed.), *National Security Strategy*, New York: Praeger.

Tellis, J. Ashley (2001), *India's Emerging Nuclear Posture*, Oxford: Oxford University Press.

Toffler, Heidi and Alvin Toffler (1993), *War and Anti War: Making Sense of Today's Global Chaos*, New York: Warner Books.

United Nations (2002), *UNCTTRAL Model Law on Electronic Signatures with guide to enactment 2001*, United Nations Publications, E.02.V.8, New York.

Waltz, N. Kenneth (1979), *Theory of International Politics*, New York: McGraw-Hills.

Zagare, F.C. and D.M. Kilgour (1993), "Asymmetric Deterrence", *International Studies Quarterly*, 37 (1): 1-27.

------------------ (2000), *Perfect Deterrence,* Cambridge: Cambridge University Press.

Zoppo, E.C. (1966), "Nuclear Technology, Multipolarity, and International Stability", *World Politics*, 18 (4): 579-606.