RUSSIA'S CYBER WARFARE STRATEGIES (1991-2011)

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

MASTER OF PHILOSOPHY

SHOBHNA KUNWAR

CENTRE FOR RUSSIAN AND CENTRAL ASIAN STUDIES

SCHOOL OF INTERNATIONAL STUDIES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI- 110067

INDIA

2012

JAWAHARLAL NEHRU UNIVERSITY

School of International Studies
New Delhi - 110067

Tel. : 2670 4365
Fax : (+91)-11-2674 1586

Centre for Russian and Central Asian Studies

12 July, 2012

DECLARATION

I declare that the dissertation entitled **"RUSSIA'S CYBER WARFARE STRATEGIES (1991-2011)"** submitted by me in partial fulfillment of the requirements for the award of the degree of **MASTER OF PHILOSOPHY** of Jawaharlal Nehru University is my own work. The dissertation has not been submitted for any other degree of this or any other University.

Shobhna

SHOBHNA KUNWAR

CERTIFICATE

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

A.K.Patnaik

Prof. Ajay K. Patnaik

(CHAIRPERSON)

Chairperson
Centre for Russian & Central Asian Studies
School of International Studies
JNU, New Delhi - 110 067

A. Upadhyay

Dr. Archana Upadhyay

(SUPERVISOR)

ASSOC. PROFESSOR
Centre for Russian & Central Asian Studies
School of International Studies
JNU, New Delhi - 110 067

Contents

Acknowledgment

Firstly, I would like to express my deep gratitude to my supervisor Dr. Archana Upadhyay. This work would not have reached fruition were it not for her guidance. Her suggestions, critical comments, and constant support have been helpful in setting the right perspective towards this academic endeavour.

I am also thankful to the Centre for Russian and Central Asian Studies, School of International Studies, Jawaharlal Nehru University, and all its faculty members for their suggestions, critical comments, and ideas that have helped me in shaping my understanding. I am also thankful to the staff members of the Centre for providing help from time to time.

Words of thanks also go to the Central Library, Jawaharlal Nehru University and IDSA library for providing sufficient reading material to me for writing this dissertation.

My friends and seniors have also been helpful to me and have bestowed their faith in me and my hard work. Therefore, special thanks to seniors- Swati ji, Sant Prakash, Saurabh, Rahul, Lalji, Shraddha, Sushant, Sameer and friends- Meenu, Neeti, and Poornima .

Finally, I am highly grateful to my family members for their unconditional love , affection, support, guidance and their unstinted belief in my capability to do well in my pursuits.

Shobhna Kunwar

Abbreviations

3-D	:	Three- Dimensional
ARPANET:		Advanced Research Projects Agency Network
BBN Corp	:	Bolt, Beranek and Newman Corporation
BESM	:	Bystrodeistvuiushchaia Elektronnaia Schetnaia Mashina
CAIDA	:	Cooperative Internet Data Analysis
CIA	:	Central Intelligence Agency
C2	:	Computerised Command and Control
C3	:	Command Control and Communications
CNO	:	Computer Network Operations
DARPANET:		Defence Advanced Research Projects Agency Network
DDOS	:	Distributed Denial Of Attacks
DECNET	:	Digital Equipment Corporation Network
DNA	:	Deoxy-Ribonucleic Acid
DNS	:	Domain Name System
E-mail	:	Electronic Mail
EW	:	Electronic Warfare
F.B.I	:	Federal Bureau of Investigation
IBM	:	International Business Machines
ICT	:	Information and Communication Technology
ICANN	:	Internet Corporation for Assigned Names and Numbers
HIS	:	Hackers Sabotage
IMP	:	Internet Message Processor
IP	:	Internet Protocol
GPS	:	Global Positioning System
KGB	:	Komitet Gosudarstvennoy Bezopasnosti
MESM	:	Malaya Electronnaya Stchetnaya Mashina
MIT	:	Massachusetts Institute of Technology
MUD	:	Multi-User Dungeon

NASA	:	National Aeronautics and Space Administration
NATO	:	North Atlantic Treaty Organisation
OECD	:	Organisation for Economic Cooperation and Development
PC	:	Personal Computer
PSYOPS:		Psychological Operations
PLC	:	Programmable Logic Controllers
RMA	:	Revolution in Military Affairs
R&D	:	Research and Development
SCADA:		Supervisory Control and Data Acquisition
SNA	:	System Network Architecture
SUV	:	Special Utility Vehicle
TCP	:	Transmission Control Protocol
UCLA	:	University of California in Los Angeles
USA	:	United States of America
USSR	:	Union Soviet Socialist Republic
WSIS	:	World Summit on Information Society
www	:	World Wide Web

List of Tables and Figures

Page No.

Preface

It is an accepted wisdom in strategic and security circles that the nature of warfare and security threats are closely connected, and therefore, a birth or emergence of new kind of threats has often led to the creation of new modes of warfare at various points of time .The Post-Soviet Period is one such period, in which changes are taking place in security and warfare areas. One of those obvious changes has been the 'enlarging of the concept of security threat'. Countries no longer see security threats as pertaining to territorial and sovereignty related concerns only, nor are they fighting the new kinds of threats with the old modes of warfare. The change in types of threats has seeped into change in modes of warfare, and almost every kind of new threat has resulted in some development of a corresponding mode of warfare to fight it.

Therefore, it is important to analyse the emergence of a new mode of warfare like cyber warfare in the context of a new developments in science and technology and increasing reliance of countries on cyber networks. The global cyber networks have empowered the humanity, but have made it equally vulnerable to some sort of invasion or disruption of networks. In recent times, more and more countries have begun to perceive these as acts of cyber war being waged by both state and non-state actors. A realisation has dawned over many countries that the global cyber network that connects the parts of the world has many open doors and gaps that are vulnerable to worms, viruses , malwares etc, a fact which enhances the deniability factor), and is a potential theatre of war.

Therefore, for Russia, which is a significant player in world politics, such a scenario holds importance from military point of view. Like any other actor with dependence on cyber networks, it is highly vulnerable to attacks. In this context offensive and defensive cyber warfare strategies and an optimum balance between the two is what can offer Russia both the fighting weapon and the guard. The offensive strategies are likely to be used in times of tensions, to create chaos in the opponents camp that would leave the latter bruised for some time. And the defensive strategies are definitely meant for

protecting one's own networks and for projecting a favourable picture of Russia.

But the word Cyberspace has spawned many phenomenon and their corresponding terms – 'cyber theft' , 'cyber crimes' , 'cyber terrorism', 'cyber power', 'cyber espionage' 'cyber warfare', and so on and so what. The meanings and content of these terms do often overlap, depending upon context. Russia, today confronts nearly all these phenomenon. But the proposed study, here, seeks to study the cyber warfare strategies of Russia as a state actor, and so, the study is bound to have military connotations.

Rationale and Scope of Study

The literature is unequivocal in presenting a scenario of militarisation of cyberspace. Militarization of cyberspace implies that states are making various kinds of efforts to anchor their controlling power in a sphere which cuts across borders, nationalities, and sovereignty. The differences lie in cyber warfare strategies, because they define the nature of control that a particular state seeks to have. This implies that countries make cyber warfare strategies to suit their needs that might pertain to power, security, diplomacy, etc. Russia is one the oldest players in the area of cyber warfare. In the current literature, it shares an equal space with China and United States. Its approach has been described as an Information warfare tactics, but very little has been said about the budding and evolution of cyber warfare strategies of Russia. The relation between the current strategic thought and the formation of cyber warfare strategies is missing in the large body of works. So, this is one of those areas that is worthy of deep exploration. There is a need to see beyond the existing literature in order to fill the gaps that the current literature has.

The proposed study seeks to pick up the thread where the currently available literature has left it. In the form of work of Azanov and Dadanov titled *Instrumental Correction for a Definition of Cyber war*, a beginning has been made in the direction where one can analyse the reasons for the multiplicity of definitions of cyberspace and cyber warfare. The two have explained how the usages of the terms like cyber war, netwar, and information war have evolved with the period of time. The independent variable in their study has been development in field of science and technology, and therefore the use of

the terms follows an S- Curve pattern, which means that the use first increases at an increasing rate, then at a decreasing rate, and finally it reaches the stage of plateau. The proposed study does not seek to do a theoretical study of the sort that Azanov and Dadanov have done. It takes the cue from the existing work and studies two relations – relation *between strategic thought and the formulation of definition of cyber war*, and relation between *developments in military science and emergence of cyber war as a new mode of warfare that is conceptually autonomous from the Information warfare*, both in case of Russia.

Secondly, this study seeks to deal with the question- Does Cyber warfare have a logic and principles of its own , or is it an instrumental appendage of the much bigger Information warfare, ? This question is significant because it is ultimately related to the other significant issue of 'Can Cyber war be counted among revolution in military affairs', or is it mere innovation?' But, why should one put emphasis on *cyber warfare strategies*, instead of focusing on just *cyber warfare*, or even on *cyber warfare tactics*? It is because strategy as a concept is neither as broad as cyber war, nor as minute as tactics. Tactics are local and immediate response to the situation, while cyber war is a very broad theatre. The study of cyber warfare 'strategies' is more helpful in revealing the relations that are to be studied here because both the technology and thought unite to achieve the goal in warfare at the level of strategy . The two relations that are sought to be studied are revealed clearly at the level of strategy. Also, the revolutionary in military affairs can be said to have occurred only when the change has come about at least at the level of strategy. The study therefore avoids making the analysis too farsighted or near sighted, by keeping strategies as the subject of analysis.

Research Methodology

The proposed study picks up two relations -the relation between strategic thoughts and the way definition of cyber warfare is formulated, and relation between science and technology and the emergence of cyber warfare as a conceptually autonomous mode of warfare. For the purpose of analysis, the variables need to be further streamlined. Therefore , for the analysing the first one, the study takes two variables to study the

causal relation between the two -*centrality of Information warfare in achieving victories in war in Russia's strategic thought* as independent variable , and the *integration of concept of cyber warfare within Information framework* as dependent variable . Similarly, the second has – *the growth in applications of Information Technology in defence sector* and i*ntegration of cyber warfare strategies in the Russia's warfare doctrine.*

The purpose of having the first set of variables in the hypotheses is to firstly examine the effect of a factor other than what Azanov and Dadanov have taken that is development in science and technology on the formulation of semantics of the definition of cyber warfare, in the context of Russia. The second set of variables is aimed at scanning the conclusion that the two scholars have arrived at, again in the context of Russia. Therefore, the study is not aimed at giving a generalised conclusion. Working on an area helps, here, in only checking a given conclusion in a given context. The third hypothesis is aimed at looking for the phenomenon that is militarisation of cyberspace. There can be many independent variables for such a purpose. This study chooses to take just one variable- efforts *to control cyberspace as an independent variable*, and thereby excluding an exhaustive analysis.

Finally, this is not a quantitative study. The information will be derived from both primary and secondary sources. The primary sources will include sources like government reports, interviews of prominent personalities, speeches, archives, while the existing literature that consists of books and journals will constitute the bulk of the secondary resources.

Chapter 1

Cyberspace: A New Security Environment

The things around us are often so familiar and known that they do not arouse one's curiosity, thanks to the knowledge that has been passed to us through various ways. The humanity lives in a kind of self-assured state, where things are familiar, or are familiarised. Animals, wild and domesticated, rivers, mountains, machines, weather phenomenon, diseases, conflicts, economy, directions, and even to an extent the near outer space where the satellites float are familiar. However, if a strange creature grows somewhere and over a course of time develops wings, hands, eyes, body hair, uproots itself, and begins to walk and fly, and hunt the human beings, then human mind will be pushed to think. People are likely to scratch their heads if they get to see such a creature. Some might call it a bird, some a hunting tree, or some might even attribute such a phenomenon to divine intervention.

The various branches of knowledge have so far not come across this kind of unfamiliar phenomenon, but they have often been compelled by the need of knowing the unknown to extend the borders of knowledge, and to familiarise the unfamiliar on the basis of what the humanity already knows. Today, a part of humanity faces a situation that is so familiar, yet so unfamiliar in various ways, just like the creature that has got the looks of a tree, human being, and bird. The machine called computer is so familiar to many on this earth. They take commands, calculate, process, run operations, entertain, and bring both wanted and unwanted acquaintances and friends to us, just with the help of a click. Apart from this, they are an unmatchable companion for many, and are the veins of the economies. People might not have time for their human companions, but they have enough to spare for their laptops. Looking at the screen of their laptops seems to give some people a kind of pleasure that one gets by looking into the eyes of one's beloved, and for those with dark interests, it is a pawn for doing nefarious activities. Therefore, a large part of humanity is in a situation where PCs, laptops, and computerised system *rule* and *run* their lives.

This situation in the eyes of many discerning people has become something like the creature that has already been introduced here. They have found something strange about it, something that does not seem to fall in the line of familiarity. Awed by its strangeness, they have given it various names –*cyberspace*, *blogosphere*, *information network*, *and internet.* This is one of the reasons why the new situation has attracted multiple understandings and varying semantics. This chapter chooses to go for the word cyberspace for two reasons. Firstly, when the literature is offering so many terms, it is not possible to do justice to all the options. Secondly, it seems appropriate at least from the point of view of semantics to use a word that matches the term cyber warfare. This, however, does not mean that the chapter will turn a blind eye to other terms that have been imparted to the same situation due to differing reasons. It is now time to look at the new creature.

Cyberspace: Forms and Dimensions

It is essential to know how cyberspace has been described. Description includes whether it has been perceived as a three dimensional[1], or with more than three dimensions or constituting a new dimension in itself, as amorphous or with definite form. Gumpert and Drucker seem to have given their part of the answers, on the basis of an argument that has more to do with Mobile Communication, than the cyberspace. But since computers are part of mobile communication, so the meaning that they seek to convey acquires relevance automatically for knowing the three dimensionality or unique dimensionality of cyberspace. The two believe that when the mobile communication becomes such that it gives a sense of mobility from one place to another without actually transporting people in the physical space, or in other words when people are able to transcend distances in physical three dimensional space, then this very sense of mobility becomes a space in itself, which creates a sense of 'everywhereness'[2] (Gumpert and Drucker 2007).

[1] Physical objects from real life are geometrically represented as three dimensional objects. So, three dimensionality, here, implies the physicality of the object.

[2] The title of work of Gumpert and Drucker is *Mobile Communication in the Twenty –First Century or "Everybody, Everywhere, At Any Time"*. The expression 'everywhereness' has been used by the authors in the context of the implications of the modern communication devices of this century's past one decade. The authors have made two assumptions. One is an implicit assumption and the other is an explicit one. The implicit assumption is that it is the idea and the perception of mobility that makes mobility or immobility possible, rather than the actual mobility in the physical space. The explicit assumption is that mobility depends upon the type of communication devices used. On the basis of these two assumptions , they have argued that the modern communication devices and systems have brought about a kind of mobility which creates a simulation of being present everywhere.

What is relevant for the understanding of cyberspace, here, is the capacity of three dimensional physical spaces to create a new space that defies the fundamentals of physicality. Cyberspace, therefore, from a perspective of communication, is a space, something psychological that gives *sense*, if not *sensation*. However, Gumpert and Drucker convey a very overarching argument that only says that if computers facilitate mobile communication, then they become a facilitator in creation of a new space that interferes with the physical space. The questions pertaining to dimensionality of cyberspace per se remain unanswered. It is therefore now necessary to look even more closely at the cyberspace, from a perspective that discusses its dimensionality.

Elizabeth Reid brings to light this dimensionality factor in a nuanced manner. In her opinion, cyberspace is a virtual[3] world, and she defines virtual world, as an interface of the psychological construct and the technology generated representations. In this context, she writes-"The illusion of reality does not lie in machinery itself but in the user's willingness to treat the manifestation of their imaginings as if they were real." (Reid 2005: 109). When the word illusion is used to describe the cyberspace, it appears illusory, and completely devoid of the physicality. However, that is not the understanding that she offers, because in her understanding, cyberspace is something that comes up when the mind interacts with the representations created by the technology called computers. It, thus, becomes evident that it is not three dimensional, yet it has something to do with the three dimensional physical world. But, strangely the cyberspace that one gets to see through the understanding of Reid is actually a virtual world, where people create and live the identities that do not exist with them in their physical, real existence. In Reid's opinion , the space called 'virtual world' is not a miracle of machine, which is a sound argument because without human imagination, computers are just as good as calculators, SUVs, elevators, and so many other things that are now part of urban life .

Reid's opinion has a bearing on how one sees the cyberspace. If it is only the virtual world that constitutes the cyberspace, then the latter cannot have three dimensional

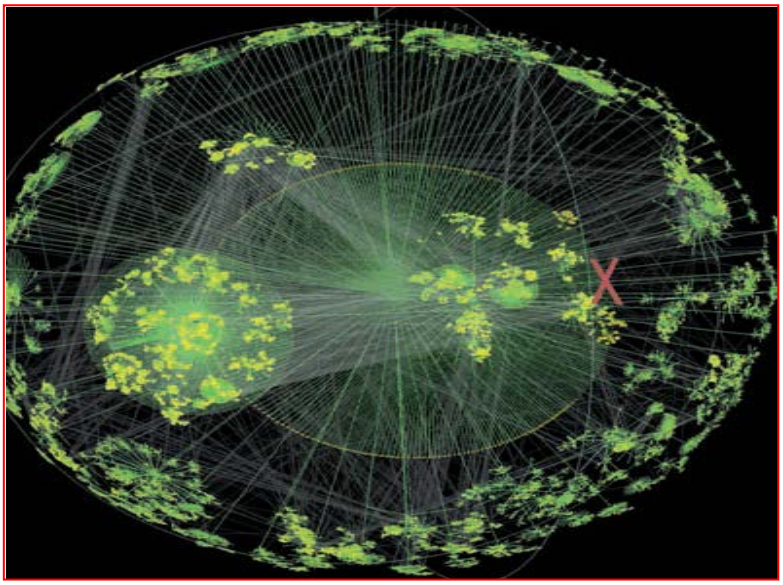
[3] Virtual means opposed to real, physical existence. It also means simulation of reality with the help of machines.Reid's emphasis is on the virtuality factor.

physical features. This conclusion however does not gel well with the fact that there are some of the physical features that are part of the cyberspace.

Mapping of Cyberspace

In order to know whether the cyberspace is all about virtuality, it is necessary to look at how the mapping of the cyberspace has been attempted in the literature, because it is essential to know the physical things that have been represented in the maps. Fortunately, there are good number of maps by now that can provide enough clues to the query– how does cyberspace look like? Some of the illustrations of various attempts to map the cyberspace are given below.

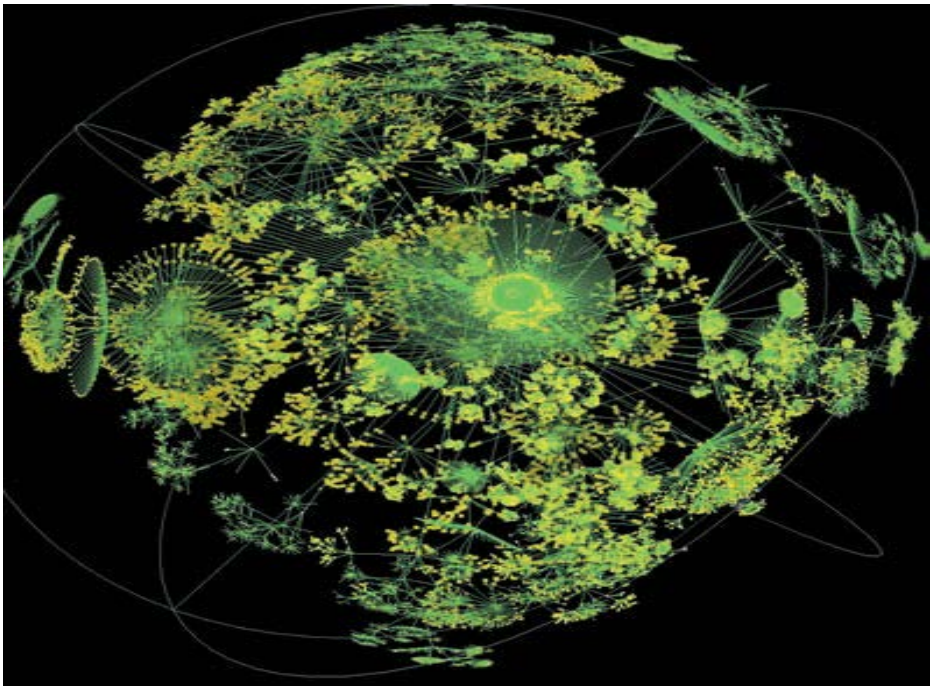
Figure No. 1.1: 3-D Visualisation of Structure of Internet



Source: *Dodge, Martin and Kitchin, Rob (2001), Atlas of Cyberspace, p.48.*

The Figure:1.1 shows the 3-D visualisation of structure of internet routing inside a sphere, made by Young Hyun. The picture in Figure:1.2 also shows the 3-D visualisation from the same source (Dodge & Kitchin 2001: 48).

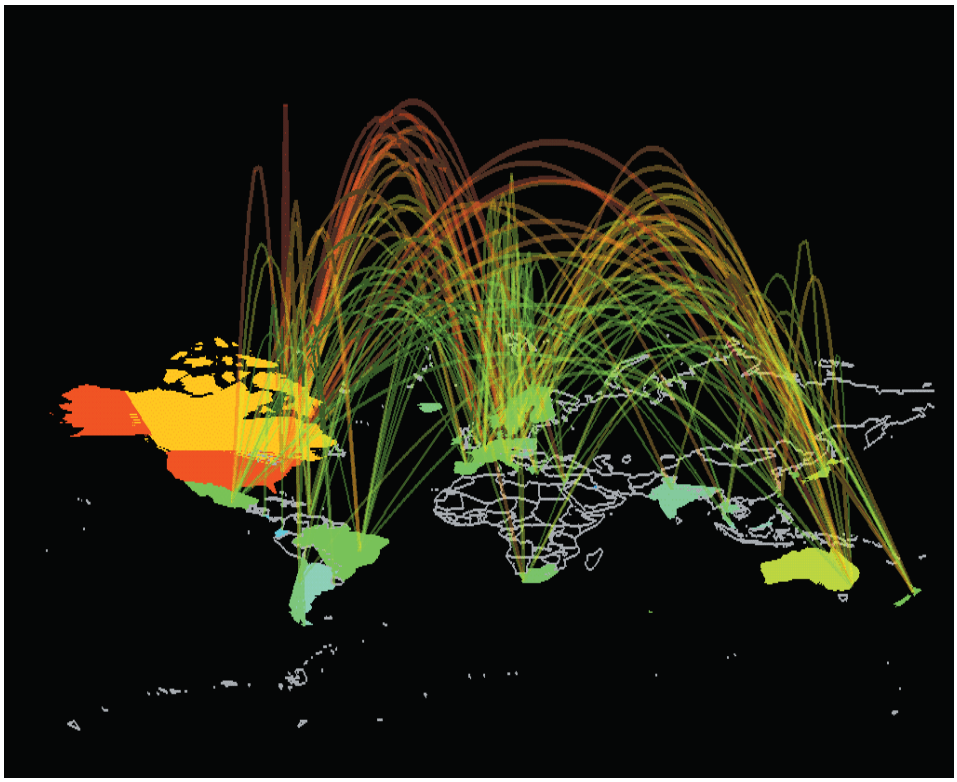
Figure No. 1.2: Another 3-D Visualisation of Internet



Source: *Dodge, Martin and Kitchin, Rob (2001), Atlas of Cyberspace, p.48.*

The chief cartographer of this and the above map is Young Hyun of Cooperative Internet Data Analysis- CAIDA.

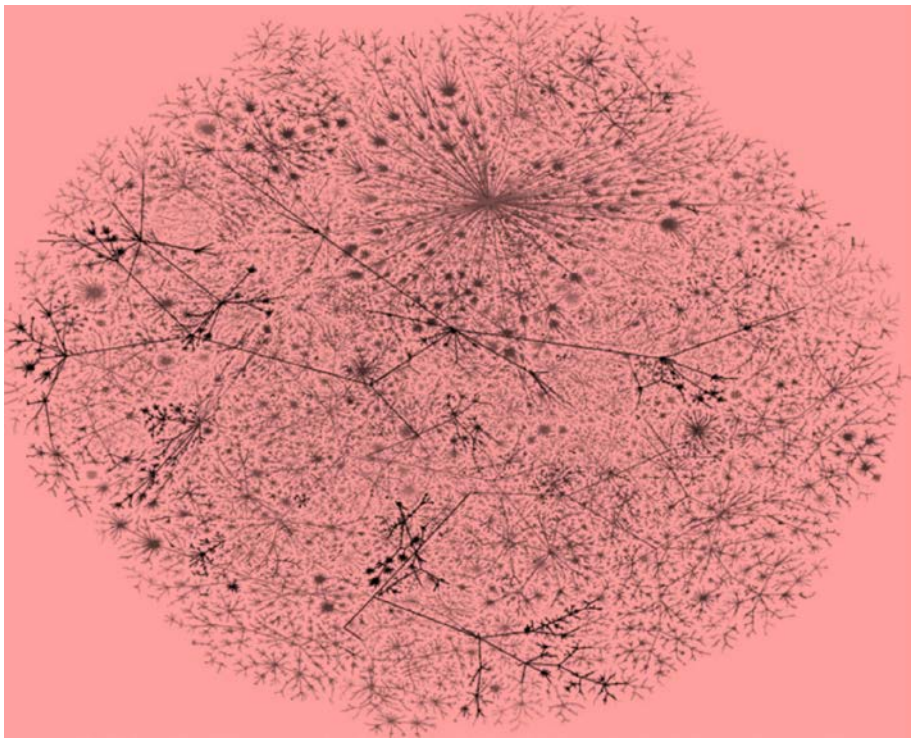
Figure No. 1.3: Network Data Flows



Source: *Dodge, Martin and Kitchin, Rob (2001), Atlas of Cyberspace, p.59.*

The chief cartographers of this are Stephen Eick and Ken Cox, Taosong He and Graham Wills of Bell Labs- Lucent Technologies. It depicts the network data flows.

Figure No. 1.4: Peacock Map of Internet



Source: *Post, David G. (2009), In Search of Jefferson's Moose: Notes on the state of Cyberspace,, p.25.*

This is a famous Peacock Map of Internet by Hal Burch & Bill Cheswick of Lumeta Corporation.

The Peacock Map, according to its makers represents the physical layers of Internet. Each line in the diagram represents a physical connection between individual networks. The individual networks have been shown as points in the map, and the physical connections that the makers have depicted through dark points are optic fibres, wires, or electromagnetic spectrum. The remaining three maps that precede the Peacock map are 3-D visualisation of the internet flow. The purpose of these maps has been to capture the picture of the cyberspace with the help of the aspects that can be represented. For instance, the three maps attempt to provide a picture of cyberspace by putting in 3-D visuals the traffic flow in the internet network. These maps do not capture the psychological part that gives the humans the very sense of

presence of a space, because human thoughts fall in subjective realm. Even maps are not likely to be free from subjectivity.

On the subjective nature of map construction, David Post writes-"Mapping is a process of creating, rather than revealing knowledge. Throughout the process of creation, a large number of subjective –often unconscious decisions are made about what to include and what to exclude, and how the map will look, and what the map is seeking to communicate. Maps then are situated, embodied, and selective representations." (Dodge & Kitchin 2001:3). If maps are situated, embodied and selective, then is there a possibility of there being one map of the cyberspace? No, because there can be as many maps as number of makers and number of meanings attached to the word cyberspace. Even here, the chapter has shown four different maps, and not one of them is same as the other one. Even though all of them seek to represent some physical attribute of cyberspace, there are visible differences in the areas of dimensions. All of them are fascinating, but each tells a different story about cyberspace. Therefore, it is difficult to say that there can be one, all encompassing picture of cyberspace. The representations by various map makers, of one physical attribute, are likely to differ from one another.

The discussion on mapping of cyberspace began with a clear, avowed intent of seeking to know whether the cyberspace is all about virtual space or is it the physical attribute, or does cyberspace consists of both at the same time. The discussion on mapping has brought out the fact that there are physical features which can be mapped. Mapping would not have become possible without some physical features. Thus, physicality is one element while virtuality is the other element of cyberspace. However, it is important to note that virtuality belongs to faculty of imagination, and it is at least as variable as the representations of the physical attribute of cyberspace. It is difficult to map it by including and excluding the visible, physical attributes on the basis of one's whims and fancies .This implies that there is not a single virtuality, but many virtualities. Therefore, cyberspace is neither *only* the physical nor *only the* virtual, but *both at the same time*, whose physical and virtual *attributes* can be *represented* in various ways. In this, it is important to remember the word that Reid has used for defining the virtual world – the *psychological construct*. The word 'construct' denotes the fluidity in the meaning.

The above discussion is significant because the attempt to study the nature of cyberspace is going to be futile if one limits oneself to only the physical or only virtual attributes. Also, it is necessary to rule out that there is one representation. In fact, the discussion in the preceding few paragraphs, gives the assumptions and the logics on the basis of which the nature of cyberspace will be studied here.

Characteristics of Cyberspace

It is easier to study something that is concrete and physical, than something like cyberspace which is both virtual and physical, because the concrete and physical stands before the eyes of an observer, while the virtual cannot be easily subjected to one representation. For this reason, a study of nature of cyberspace requires going beyond the representation of physical attributes in order to see what actually goes on in cyberspace. In other words, the various manifestations[4] are crucial to such study than just the wild goose chase for one sole representation that shows different parts of the cyberspace. Therefore, to begin with, it is important to describe the players, or actors or participants in this cyberspace, as opposed to just one player or actor.

Cyber Actors

One of the significant characteristics of cyberspace is cyber actors, who form a human dimension of the cyberspace. The 'cyber actor' has become a phenomenon, and a generic term for a *human physicality that has got disembowled* .According to Tim Jordan, Cyberspace has been a means of empowerment to those who can participate in it. It enables them to create their own society, their multiple identities. They love to be in multiple identities. The physical world embodies the human, it shackles the human to a uniform, unbroken identity, and the cyberspace releases them from those shackles. Jordan has cited the instance of a neuropsychologist who became paraplegic after an accident. Left with a body that made her feel so miserable, she fell into depression and decided to commit suicide. However, a friend gave her a computer, and high level technology that could enable her to communicate with people online. And from then onwards her journey became not just comfortable but also exciting. She gave herself the identity of a girl called Julie, who is young, flirty, beautiful, and who loves to romance men. After that, Julie made many close friends online,

[4] The manifestations, here, means the activities of cyber actors when they are online and its consequences.

romanced men, both young and old. But she decided to never meet her online friends face to face. Her husband who had been typing for her, kept the identity alive. But, somehow a person managed to find out the place where Julie lived, and then the identity of Julie was unravelled. It was the neuropsychologist's husband, who had been living the life of Julie online. Many felt cheated, and were aghast at the discovery of the Julie they had been romancing online (Jordan 2003: 63- 66).

The point that Jordan has tried to emphasise is that the cyber actors have the immense power to manipulate and play with their identities, resulting in a situation where the identity transforms from seamless to a fractured one**.** In fact, according to David Hakken, it is cyborgs[5] that create their social world called cyberspace. Jordan has given agency to the cyber actor and the machine only, and so has Hakken but the latter is sceptical about the theories that seek to emphasise a lot on the computer revolution, and its impact on human beings. His focus is on the way the cyborgs create the cyberspace, that is the agency of cyborg. He seems to be even uncomfortable with the use of the term cyberspace , because according to his argument cyberspace is not something that appears to be lying out of the community that cyber actors create (Hakken 2002: 15-19). Therefore, important point is that world also consists of cyber actors, who are *much more liberated* than the ones who are not in that category, in the sense that they *can manipulate* their identities.

Activities in Cyberspace

Cyberspace has made innumerable things possible. With the arguments given by Jordan and Hakken, it has already been mentioned that the foremost common activity of cyber actors is creating a cyber society of their own, where they can live the lives of multiple identities. The above discussion that dealt with the cyber actors indicates both a broad and a narrow picture of the activities in cyberspace. It indicates a broad meaning because all the cyber actors engage in creating their cyber society .On the other hand, the meaning is narrow, because there is more to cyber activities than mere creation of cyber communities. The way communities interact with the cyberspace environment also defines the various shades of the cyber activities.

[5] The term *cyborg* was coined by Manfred Clynes and Nathan S.Kline in their article *Cyborgs and Space*, which dealt with the concept of self-regulating human machines in outer space. Later D.S. Halacy popularised it further by dwelling on it in his book *Cyborg: Evolution of Superman*. It is now used for an organism that has enhanced capabilities due to advanced technologies.

For instance, according to Harvey Jassem cyberspace has become not only a space for connecting with each other, but along with a social space it has also become a resource for exploitation. It has become a resource for people who commit cyber frauds. Jassem , here, gives many instances of cyber thefts and the ways those thefts have often occurred. One of the thefts he talks about is the cyber financial fraud , which involves theft of secret details like credit card numbers, of people who fall into the trap of *phishing* and *pharming* (both the methods are used for tricking the naïve users into giving secret details related to bank accounts) Jassem also talks about cyber-violence, which could happen in the form of a derogatory remark made against a person in online, or through display of violent, racist , sexist, pictures , words, speech, photos etc, or through use of electronic media to pursue or harass a person . The virtual world has become the place where these perpetrators of cyber violence operate with great impunity (Jassem 2007: 98- 101). Therefore, cyberspace can be as discomforting as the physical world. It is not a refuge for people for who seek to run away from the nastiness of the physical world, rather it can be as full of dangerous locations as the physical world, where theft is as easily possible as it is in actual physical existence. In fact, according to Mc Afee report on virtual criminology, cyber criminals know how the helplessness of people in the current global scenario compels them to be online. People simply cannot remain out of cyberspace, because it is a gateway to so many opportunities. They become vulnerable to duping, which makes them a very easy prey for the cyber thieves, who are on the lookout for some good resource to get rich quickly. On the other hand, the means that cyber criminals use are untraceable. They have developed new ways to launder illicitly gained money, which are more easily applicable in developed parts of the world due to the widespread use of high technologies (McAfee Report: 5-7).[6]

It is therefore obvious by now that what is called cyberspace has not only come into being , but has developed a tendency by which it is becoming crowded and transforming into a space that is easy to exploit for various purposes. And here comes the point, where it is necessary to discuss the challenge that the state actors face due to the coming into being of a space, a domain that is part virtual, and part physical,

[6] See McAfee Report Virtual Criminology Report: Cybercime versus Cyberlaw, McAfee Inc. URL: http://www.ifap.ru/pr/2008/n081212b.pdf.

and is actual. The vast physical world is so easy to function in for the state actors. Everything is right before their eyes, even the outer space. There are border disputes that are irritants, but at least they can see where things are, what is lying where. There are conflicts, whose physical and psychological manifestations they can see and perceive. If there is an ethnic conflict, they can see it. If there is a conflict between ideas, they can still see it. In the space where the state actors live and flourish, things have borders, and opponents are so visible. However, the emergence of cyberspace has thrown the state actors into confusion. It has given rise to challenging situations for the state actors in the areas of security and warfare. These questions are important for tracing the reasons for the coming of concept of cyber warfare in the military doctrines of a number of nations. The following section explores these questions.

Cyberspace and State Actors

The principle on the basis of which cyberspace has come into being and grown has been the unique combination of virtuality and physical world. The flow of ideas and information have been taking place since ancient times , and that is how so many changes could happen around the globe , and that is how the world could come to this stage where it is now. Ideas flow in cyberspace as well, but what sets it apart from an ordinary domain where information flow is the factor of virtuality, which (as has been seen) relies a lot on the human imagination, its manifestation, and its perception by others. The very power of virtuality has been manifested in the way it has sucked the physical world into it. This sucking process has been facilitated by the explosive growth of the Internet. David Post gives the figure of internet host machines, that from December 1969, when there were only 4 hosts in the globe, it has grown to 541,677, 360 in January 2008 (Post 2009: 31-33). On this process of sucking , Daim Shabazz says that the explosive growth of internet has brought about a new order which has given individuals , institutions and governments an easy access to information , and the rigidly defined borders are giving way to the virtual communities, and netiquette (net etiquettes), resulting in the deterritorialisation of the globe. Today's world has quite a number of 'virtual states'. In this context, Paul Frissen has also driven the point that the coming of ICT (Information Communication Technology) has led to freedom from some shackles that the organised, vertical organisation of state actors provide. The world is more local, multi centred now. The centralised organisation of state is relevant where time space constraints exist, but the

ICTs have reduced those constraints, resulting in a more localised world, a more deterritorialised world (Frissen 2005: 116-120).

Therefore, for the state actors, cyberspace is a new environment they have to live in, and a new challenge that they have to take on. Countries are already aware of this fact, about this growing space that has sucked various parts of the globe into it. For instance, Stuart Biegel describes the confusion that state actors are facing because of the dawn of cyberspace, in the legal matters, in prosecution, trial, and evidence, and even the very definition of crime. In his opinion, cyberspace has not been defined in one definite way, which creates more hurdles in the legal matters. He has cited one instance called Reno *VS* ACLU litigation 1996-97, in which the deputy solicitor general representing United States federal government argued that Internet was basically a library, while one of the judges said that it was more like telephone (Beigel 2001: 26). The sort of confusion that Biegel has referred to is bound to create more challenges for the law enforcement and justice system of the various countries. In fact, Biegel has titled his book (which contains this particular instance) as *'Beyond Our Control?'* Here, it is important to use the analogy of the strange creature, which was talked about in the beginning. Today, the cyberspace is more like that strange creature. It is visible to the eyes, everybody sees it, and perceives it differently and defines it differently, creating more confusion for the state actors, who had hitherto been dealing with the problems that had nothing to do with this kind of space or domain.

State-actors find the control over the cyberspace and its governance to be the most challenging aspect of the cyberspace, primarily because of the fact that it remains *undefined.* Therefore, it is appropriate to discuss the debate over the *definition of cyberspace.*

Definitional Discourse on Cyberspace

State actors, today, feel almost baffled, puzzled, and are in quandary, primarily because despite seeing it, the humanity has still not settled on one definition. A clear, coherent, uniform definition that they need in order to overcome the confusion and the fragmentation that has happened as a result of the multiple definitions still evades them.

In fact, ever since this term cyberspace was conceptualised by William Gibson in his fictional work *Neuromancer,* multiple conceptualisations have taken place. In this context, Loader appropriately says that the definitions of cyberspace are so diverse that now it is a curious mixture of science fiction and others that have come later. As a result of this, while analysing this domain or space, one is not able to tell that what exactly has to be analysed. Definitions are many, but are not necessarily inclusive of all features of cyberspace For instance, there is a cyber libertarian perspective of John Perry Barlow and others, that seeks to define cyberspace as an electronic domain, that is virtual, homogenous, and is free from the shackles of state, sovereignty, nationalism, and militaries. According to Loader, such a conceptualisation of cyberspace has its own limitations- firstly; it is a very narrow conceptualisation, because of its overemphasis on the virtual aspect. Secondly, Loader has pointed out the fact that the cyberspace is not completely free from the state control because the infrastructure of ICT (Information and Communication Technology) is largely controlled by the state, in most of the countries. Thirdly, he says that cyberspace cannot be assumed as homogenous space, because the global space does not have uniformity (Loader 2005: 2-7).

Therefore, Loader has brought out the debate on defining cyberspace in the open. This debate exists due to the inability of scholars to incorporate the dual characteristics of cyberspace- its virtuality and its physicality. Biegel, who has already been referred to in this chapter in a similar context, gives a slightly different twist to this dilemma which affects the scholarly community in agreeing to have a consensus on one definition. But before, one jumps to see what Biegel has got to say, it is important to discuss his view in the context in which he says. Biegel begins the discussion on cyberspace with the implications of cyberspace for the legal community. He brings in the varied ways in which different members of the legal community that includes lawyers, judges, scholars, comprehend cyberspace and define. But, what is so significant in what Biegel does is not just his attempt to discuss from a legal perspective, but his success in bringing to light a category of opinion that believes that there need not be one definition of cyberspace. He calls the category- *moderates,* and sums up the view of this category by saying-"Proponents of this view argue that at a certain point, it is only logical to refer to the place where all this is happening as a different place. It may be different conceptually, or it may be different legally, or for

some, it may even be different physically." (Biegel 2001: 25-38). The one reason he attributes to for the growth of this category is the different ways in which people have experienced cyberspace.

What Biegel has brought to light is borne out by the fact that the cyberspace has acquired so many forms and made so many things possible that it itself has undergone some sort of fragmentation, before scholars could even reach a consensus on what the cyberspace means . An individual, sitting with his or her laptop, connected online with a friend experiences cyberspace in a way which might be quite different from the way a person controlling weapons system or devising a worm or a virus does in a military environment. Or, a person who is doing online shopping experiences cyberspace differently than a person who is being violent with someone online. One can call it the experience perspective of looking at the definitional debate, or the absence of one definition, which finds the cyberspace to be too fragmented to be brought under one definition. However, this perspective has its own limitations, one being that experience cannot be counted as the sole factor in defining cyberspace. If experience becomes the sole factor that should be taken into account while defining cyberspace, then firstly the cyberspace would appear to be fragmented to the extent where each individual would have his or her cyberspace, different from that of other individual. Secondly, it would reduce cyberspace to a space that is devoid of physicality, which cannot be true because cyberspace has come into being due to some physical characteristics, which have been even mapped in various ways, with the help of various technologies. In fact, assuming cyberspace as only a virtual space, which can only be experienced is like assuming that one is able to hear Beethoven's music without Beethoven, or even the recorder that has kept his music recorded.

Therefore, the cyberspace has failed to bring the scholarly communities to a point where they can demarcate it and give it a coherent single definition. Whether it is the question of how it looks, or how it is mapped, or how it has been defined, the literature is beset with multiplicities. What state –actors, therefore, see today is a space that is not only experienced variedly, but also remains undemarcated and that is where the challenge lies in the security sphere for the countries. Now, is the time to move on to the security, and military issues.

Securitisation of Cyberspace

Due to a very amorphous nature of the cyberspace, it poses a great challenge to the state actors in the security arena. This section will discuss the ways in which the cyberspace has come to pose security challenges to the state actors. It is important to note that this section is not going to discuss the challenge to the very existence of the concept of state. In other words, the section will avoid talking at length about issues that pertain to globalisation, and deterritorialisation. It has been already briefly discussed in one of the preceding sections in the context of a very conceptual kind of threat to the concept of state. Here the discussion is sought to be confined to the security threats, their nature, and how they have resulted in the formation of a new security environment. However, the task under this section precludes any kind of a discussion of cyberspace in the context of non-traditional security threats, the prime reason for this being that the cyberspace remains undefined in a coherent manner. So far, it has evaded any kind of even a general consensus. In fact, it is a new space that moves according to its own logic, that often defies the three dimensionality. Therefore, the approach here is to treat cyberspace the way this chapter has treated the strange creature - completely new, that is attracting cries of unfamiliarity.

After giving the outline of this section, it's now time to move to the security threats that the states face *in* the cyberspace. The word has been italicised to facilitate an understanding that states cannot face security threat *from* the cyberspace, because the states are already present in the cyberspace. Their very participation in it has led to the securitisation of it. So, Joyner and Lotrionte have pointed out correctly that the Western societies spent years on building the information infrastructure and improving it so that there could be more connectivity, and openness. It was these efforts that led to the Internet becoming ubiquitos, and so the consequences are obvious today (Joyner & Lotrionte 2001: 826-829). The consequences that the two are referring to are securitisation and militarisation of the cyberspace. Therefore, now there are threats called cyber security threats that had not existed earlier. Like the cyberspace, cybersecurity is also very amorphous because such threats can emanate from anywhere, any person, anything. Project Grey Goose Report, of Grey logic[7] has

[7] See Project Grey Goose Phase II Report: The evolving state of cyber warfare, dated March 20, 2009. The Report is a work of Grey logic. Project Grey Goose began in the wake of Russian cyber attacks against Georgia in 2008 during its conflict with the latter over the disputed territories of South Ossetia and Abkhazia. The project began in 2009 with the purpose of analysing role of state actors in Russian

done a series of studies on the evolving state of cyber security threats. The reports have brought out certain results and conclusions that say that the threats in the cyberspace have often emanated from the non- state actors like, primarily the hacker groups, and their performance indicates that they have the potential to wage a cyber war against targets that they identify as belonging to enemy states. The weapon could be virus, or some other malware[8] that can lead to the theft of secret codes that a security agency uses for keeping the secrecy of information (Carr 2009).

In a world devoid of a technology like that of computer and Internet which is flourishing on the basis of some free flow of information, and fast connectivity at a great speed, the kind of attacks that Carr and others have talked about could not have become possible. So, when this section at its outset said that this space called cyberspace moves according to its own logic, the sentence was referring to this kind of movement that the space creates, or rather has already created. The logic of cyberspace has brought about a situation where countries, today perceive threats from completely immaterial, non-physical, creations of the human mind and the machine – virus, malwares, and worms[9]. Therefore, in this sense, cyber security discourse that sees vulnerability at various points, to attacks from these creations is *partially* a consequence of an interaction between human mind and machines. In this discourse, nearly everything is having an open door and a window, through which threats can enter, and one will not even be able to trace it properly.

This cyber security discourse has come about only partially due to the interaction between human minds and machines. The other factor that has contributed to this whole discourse is the ever increasing attempts of state actors to militarise what is called cyberspace, which the following section deals with.

Militarisation of Cyberspace

There is an implicit assumption in the above section, towards its end .The assumption is that securitisation of cyberspace is a partial consequence of the attempts to

cyber attacks against Georgia, and has evolved into a consultancy firm that deals with analysis of cyber warfare related events.

[8] Malware is a short form of Malicious software, which consists of programming (code, active content, scripts, and other softwares), and is designed to disrupt, or deny operations, steal the secret matter, and harm the privacy. Computer virus is a kind of malware.

[9] Viruses and Worms are the types of malwares.

militarise it. Some might find that it is the other way round, that security threat leads to the militarisation. Here, this section seeks to take this only as an assumption for the analysis of the militarisation of cyberspace. This has been done to facilitate a longer and a more focussed discussion on the militarisation that is the military aspects – warfare, strategies, and weapons, and military actors. The first to be discussed here is conceptualisation of cyberspace as a new battlefield. When was cyberspace first thought of as new battlefield? It cannot have one answer because it has been an evolutionary process. It is only in this decade which has just gone that one got to hear of cyber war, without any alarm, because this was the decade that saw a real movement towards such kind of conceptualisation. United States, which is regarded as an early adopter of cyberwarfare established a cyber command in November 2006, and it was United States Air force that established it. That same year, the policy makers also developed the *National Military Strategy for Cyberspace*. This is a codification of understanding of U.S.A. of the 'cyberspace war fighting domain'. The document has defined this warfighting domain as a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures. Its first commander Lieutenant General Robert Elder Junior called it the 'Mighty Eight' command that would have cyber warfare capabilities and 'warfighting missions' (Hughes 2007:21).

The Chinese are also not lagging behind .Firstly, they translated into English their own publication, *The Science of Military Strategy,* and gave the translation of cyber attack in 2005, and after about 2 years, the *China National Defense News*, gave its own definition of cyber war**.** Further, in the same year when the Americans established their cyber command, China also came out with its document that consists of a sort of strategy and information planning for the period 2006 to 2020. It has been titled as *State Informationization Development Strategy*, which means that it does not have as strong a military connotation as the American document has got, but it still contains a security element pertaining to cyberspace. The Russians are not out of this club either. It has already learnt to use cyber warfare strategies in ordinary conflicts. In fact, like the Chinese, the Russians too have been often blamed for employing the cyber attacks against the unfriendly countries. The most recent instance of a Russian cyber offensive is the cyber attacks that Russian hacker groups mounted on the Georgian cyber networks during the 2008 Russia –Georgia conflict. In fact, Russia's

cyber offensive shook the NATO (North Atlantic Treaty Organisation) to an extent where they were forced to establish the Cooperative Cyber Defence Centre of Excellence in Estonia. The officials at the Centre have revealed that following the Russia-Georgia conflict [10]in which Georgia bore the brunt of the Russian cyber offensive, a Cyber Defence Management Authority has been set up which is a part of NATO's cyber defence policy .This is not even the full story. The NATO has taken the militarisation of cyberspace to a level where they have successfully conducted three cyber defence exercises, called Cyber Coalition since the year 2008. (Thomas 2009: 465-466, 475-481; Thomas 2009: 55-58; Myrli 2011: 89). In fact, Monica Chansoria writes –"Both the Chinese and Russians have learnt from the mistakes committed by others and have become Information Warfare forces to reckon with**."** (Chansoria 2010:10).

However, U.S., China, and Russia are not the only countries that have either incorporated cyberwarfare principles into their overall warfare strategies, or have developed the capabilities to fight in the cyberspace. Iran has its own numerous hacker communities, and groups. One such group is IHS (Iran Hackers Sabotage) .According to their account, this group was formed in 2004. So far it has targeted more than 3000 websites. On July 2005, they defaced the US Naval Station Guantanamo's public Website, and conveyed the message that Muslims were for peace, not terrorism, and that many had been harmed in Israel, Iraq, and Guantanamo. One month later, another hacking group called Ashiyane Digital Security Team defaced the NASA (National Aeronautics and Space Administration)'s website and challenged the US policy in the Middle East. So far, there is no conclusive tell tale sign that shows that these hacker groups are colluding with the state actors in Iran. However, the state is now actively pursuing the agenda of securitisation of cyberspace (Denning 2007: 200).

Apart from this, even a poor and isolated country like North Korea[11] is investing on developing capabilities to inflict cyber attacks. According to South Korean

[10] The Russia-Georgia conflict in 2008 was a military conflict that arose from the disputed nature of the South Ossetia and Abkhazia, the two territories that lie between Russia and Georgia.

[11] North Korea has remained under the single party Communist regime since 1953. It follows a policy of *juche,* which means self-reliance. This policy has prevented it from forging close economic and political ties with most of the countries. Due to these two factors, it has remained isolated from rest of

Intelligence, North Korea's hackers attend a special five year college called Automated Warfare Institute. Situated in the mountains, this military academy, according to South Koreans, produces 100 cyberwarriors per year with degrees in subjects such as automated reconnaissance. Indeed, there is even a bigger surprising fact and that is that the Automated Warfare Institute was actually established way back in 1984. At that time, it was known by the name of Mirim Academy, and used to offer a two year program in IT and electronic warfare for top military students. So no wonder, the Commander General of South Korea's Defense Security Command has claimed that North Korea's military hackers had been conducting CNO (Computer Network Operations) against South Korea's government and research institute websites to steal classified information. (Naim 2005: 92; Denning 2007: 204-205).

Therefore, regarding the fact that cyber warfare as a concept has been born, there cannot be two opinions. In fact, it is very much a part of practice, and it is not the just the big boys of international politics, who are moving towards a militarisation of cyberspace, rather the cyber warfare capabilities have been possibly acquired by even the less powerful states. The dawn of the twenty first century has seen an obvious movement towards militarisation of cyberspace. But would cyber warfare have taken place two decades back? Was the concept of the kind of cyber warfare that is heard about these days, actually born earlier? According to some the idea of a cyber war, then in 1990s, would not have been accepted as real. Vatis is one of them. On the idea of cyber war, he writes: "A decade ago, when the World Wide Web was still in its infancy, the scenarios of cyber war would have been derided as an alarmist." He further says, "Today scepticism about the cyber threat is more difficult to find. Government agencies, companies, and individuals are all too aware of the harm that computer viruses and hackers can cause." (Vatis 2006: 56). Vatis can be regarded correct in pointing this out, because even a decade back the idea of cyber warfare was not even conceptually developed. That does not imply that the concept of cyber warfare has come about in Facebooking generation only because that would amount to saying that the cyber warfare was conceptualised out of nowhere.

---

the world. However, it has some degree of reliance on two countries- People's Republic of China and Russian Federation.

For the people associated with strategic, and military circles, this is not a very new field now, because beginning of militarisation of cyberspace can be traced to a much earlier period, when the world was bipolar. It was in 1980s, in the environment of a polarised world that a journey to militarise this space began. The Soviets, at that time, did not see it as cyber warfare, but as an imminent technical revolution. In 1984, the then chief of general staff Marshal Nikolai and others observed that precision munitions[12], wide-area sensors[13], and computerised command and control (C2) were the developments that in field of non-nuclear destructive capabilities that could make it possible to increase by an order of magnitude the destructive potential of conventional weapons, bringing them closer to weapons to mass destruction in terms of effectiveness. The Soviets decided to call it Reconnaissance –strike in order to describe the integration of missiles with the precision guided missiles, area sensors, and automated C2. The Americans then did not wait for long to apply what the Soviets had already predicted and conceptualised. Ogarkov had expressed his opinion and analysis in 1984 about the utility of the new mode of warfare, and its manifestation was to occur seven years down the line. In the Operation Desert Storm, in 1991, the Americans unleashed what later came to be known as information warfare. The Iraqi electronic communication lines were disabled in a very selective manner, which proved to be really effective in making the precision guided bombs more lethal. In the latter part of the 1990s, this change was defined as a Revolution in Military Affairs. (Watts 2011: 1- 2; Cohen 1996: 39- 40).

The 1990s then became the decade of great change in the way countries thought of the very concept of militarisation and security, because everybody saw how the Americans had leveraged the power of computers to hit Iraq where it mattered the most to that country, but everybody also got to see how vulnerable the country could be due to the same technology that had helped the Americans in achieving their goal without much effort. The dependence on the Information sphere was as visible to the discerning observers as the success the United States had got. It was this that set off another arms race. But this time the race took place in another domain. It was not

[12] Precision munitions are a short form of Precision Guided Weapons. Recently, United States has heavily used these weapons in Afghanistan.

[13] A Sensor is an instrument that measures a physical quantity and translates it into signals that can be read or measured by a person or an instrument or a machine. Area sensors are deployed for a survey of an area and the physical movement there.

land, or water or air or even the outer space, but a virtual cum physical space called cyberspace. The weapons that have been devised since then are the ones that do not roar or explode or strike. They are the weapons that attack in a creeping manner, noiselessly, and slowly. So, it is easier to understand what Vatis had meant when he said that the idea of cyberwarfare in 1990s would have raised an alarm because the World Wide Web was in the stage of infancy, and the world had not connected to a great extent. Therefore, in the first half of the decade, at least, there was no possibility that countries would engage in the militarisation of cyberspace in a big way.

On the other hand, the late 1990s saw acceleration in the militarisation of cyberspace. The surprising element this time was the direction and form of militarisation. The cyberspace had begun to be militarised by the states, but there was the rising prominence of the invisible non-state actors. In the year 1998, when the anti-Chinese riots were taking place in Indonesia, around 3000 hackers organised themselves into group called China Hacker Emergency Meeting Centre, and later targeted the Indonesian government websites . One year later, when the NATO jet accidentally bombed the Chinese Embassy, in Belgrade in Yugoslavia[14], the Chinese hacker group called Red Hacker Alliance attacked the US government websites. In 2001 also, when the EP3[15] incident took place, about 80000 hackers launched a 'self defense' cyberwar with the US (Carr 2010: 2). These are just few instances of the cyberwar, although no country has ever admitted to using the hackers. In fact, the rise of non-state actors has to a large extent enabled the countries to ward off any blame of having waged a cyberwar. The kind of militarisation that has taken place and is still going on is not the type which is associated with the mode of warfare that is conducted in land, sea, air, and water. It operates on the basis of the logic that moves and expands the cyberspace.

[14] Kosovo Conflict took place in 1999. Kosovo was then a republic of Republic of Yugoslavia. The ethnic Albanians had demanded independence from the Yugoslavian Republic. An organisation called Kosovo Liberation Army was formed that espoused the cause of independence of Kosovo. The Western Countries were for the independence of Kosovo as well. So in the name of democracy and human rights, the NATO forces conducted Operation Allied Force or Operation Noble Anvil. In this operation, the air power was heavily used.

[15] In the EP3 incident US plane EP3 was operating near Chinese island province of Hainan. China's J-8 aircraft intercepted it, but there occurred a collision in which the Chinese pilot died and the EP3 had to land in Hainan.

Power Asymmetry in Cyberspace

It is important to mention that nearly all the efforts of the countries have centred around one thing, and that is the control of the cyberspace. In other words, the mechanism (about which the question has been raised here) has diverted its energy towards resolving issues that pertain to the control of the cyberspace. Here, the main issue is the tussle between United States and others over the domain called Internet. The most complex aspect of this tussle is the way it began. It started with a need to regulate and control the cyber crimes.[16] The Organisation for Economic Cooperation and Development, conducted its own study called Computer Related Crime: Analysis of Legal Policy, in 1986, which recommended some changes in the domestic laws of member countries in order to update the existing legal structure for dealing with cyber crimes. Following this, the United Nations also adopted a resolution in 1990 on computer crime legislation. But the major forward step was taken in this direction only when the World Summit on Information Society was held in two phases, once in Geneva in December of 2003, and later in Tunis, and came out with two agendas- the *Geneva Agenda for Information Society* and the *Tunis Agenda for Information Society.*[17] (Portnoy & Goodman 2009: 5-7).

What these efforts have brought to the fore is the asymmetry in the zone of cyberspace. Internet is widely and commonly seen as a zone which is perfectly autonomous, in which a poor country has as much power as the mightiest one on this earth. But in reality, far from a small, poor country possessing as much control as United States , even the relatively better off countries of the West do not have much say in the operations of the popularly called 'Free Internet'. Quite a number of countries have criticised the existing arrangement. According to Cukier, this arrangement consists of three things- domain names, Internet Protocol numbers, and the root servers.[18] The control of Internet is dependent on these three things. How? Firstly, every website has what is called a domain name. It is just like a name given to a person, and for visiting any website; the site should have a domain name. This system of assigning domain name is controlled by a body called ICANN, which

[16] Cyber crimes are not same as cyber warfare.

[17] In general, both the agendas are two parts of the same thing, and both seek to protect networks from cyber crimes, consumer rights, and privacy.

[18] Internet Protocol is the messaging format of the communications between computers and domain names are the codes that the protocol can identify for locating a information .Root servers are the programs that help in that identification.

stands for Internet Corporation for Assigned Names and Numbers. This body began as a venture under the leadership of a Computer Science Professor, Jon Postel, and it is a private sector body, which means that it is not a government department under US federal government. But that has not prevented United States from controlling the ICANN. The second factor that gives US an edge over others is the fact that it has the maximum number of root servers (root servers match the domain names with the Internet Protocol numbers which in turn are invisible to users , and are like recognition marks) (Cuckier 2005).

Basically, what Cuckier seems to shatter is the strongly held myth or belief that the cyberspace is the domain that is so autonomous that it has the potential to challenge the very concept of state, because large number of countries find Internet to be beyond their control.. This opinion also seems to rule out the possibility of state actors losing their significance very soon due to emergence of cyberspace. In this chapter, under the section titled Cyberspace and State, it was stated, on the basis of some arguments that today state actors find control over cyberspace and its governance to be the most challenging aspect of it. On the surface, such a statement appears to be quite opposite to what Cukier has said, but it is actually not. And the reason is that the cyberspace is a big challenge to the states because it has many aspects that defy the physicality, it remains without borders, yet it is space that is distributed asymmetrically. It has its own structures of power, which might or might not involve state actors.

Conclusion

The amorphous nature of cyberspace has prevented the scholars from arriving at a consensus on its fundamental definition. The reasons lie in the complex nature of cyberspace. It is not a space that is completely physical, or completely virtual. Instead, it is a unique combination of virtual and physical, which has attracted various ways to represent it, primarily because virtuality is not confined to one group or experience, rather it is a highly manipulable.

However, it is the absence of the consensus that is bringing out so many complexities of a field that is young. Had there been a consensus on the fundamentals, then there would have been confusion with the emergence of a new feature or phenomenon.

Also, there would have been a failure in understanding the really complex nature of this space which seems to defy the fundamentals of the physicality. The evolution of cyberspace is still on, and the more it is evolving, the more states are finding it tempting. They do not want to confine their participation to just regulating the cyber-crimes, but are expanding their footprints in the cyberspace. So along with the cooperative mechanisms to deal with cyber crimes, the states are actively pursuing their programs to develop their cyber warfare capabilities.

However, the approach to the concepts and practice of cyber warfare have not remained uniform across the countries , which means that despite some similarities , there are innumerable differences in how countries intend to integrate the concept of cyber warfare in their overall warfare strategies . This implies that strategies to fight a war in cyberspace differ from one country to another, depending upon how they understand the cyber warfare. This point will be dwelt upon in the next three chapters that deal with cyber warfare principles and approaches, historical contexts, and Russia's approach to this new mode of warfare. The understanding based on this chapter will help in explaining the conceptual parts of the cyber warfare, which are as complex as the cyberspace. Also, a study on the cyber warfare strategies would have remained incomplete without preliminary discussions on the cyberspace, and why it provides a new security environment to the state-actors. It's now time to move on to the next link in the chain.

Chapter 2

Introduction

This chapter is aimed at analysing cyber warfare – its definitions, principles, types, weapons from the perspective of state actors. For that, it is essential to discuss a process of evolution that has brought humanity to the point where this kind of warfare is not only being contemplated , but has also been put into practice by quite a number of state actors. This evolution holds significance because the fundamentals of a new mode of warfare, which is just a decade old, cannot be understood without looking at the previous picture. The question arises- from where should one start, in order to study this evolution? Should one go back to the Stone Age to trace the process of evolution, when the apes roamed the Earth and used stone flints to hunt and survive? After all, engaging in war has been a very ancient pursuit for humanity. Therefore, what one needs here, is that part of the evolution *that has transformed one mode of warfare into cyber warfare*, and not a leisurely walk through a whole process of evolution of warfare practices dating to the Stone Age. The first section that comes next deals with that part of the process of evolution.

Transformation in Warfare Practices: From Industrial Age to the Dawn of Cyberspace

There is a term called Revolution in Military Affairs (RMA), which has already been mentioned in the previous chapter, and has become popular only in the Post 1991 Gulf War. However, the revolution in warfare practices have taken place at various stages of the history, and the Post 1991 revolution is not the sole instance .The Revolution could be in organisation, combat, weapons, the structure of military organisation ,and structure of command. Cohen believes that the changes could emanate from the civilian technologies also. He cites the 19th transformation in warfare practices as an example of RMA. In the nineteenth century, the age of mass army arrived gradually, when the French resorted to the use of a very large army, so that the human losses could be replenished quickly. So this revolution was both organisational and conceptual. Later, when the railways and telegraph became

common, these two civilian technologies made several things possible that had not been envisaged earlier. The excellent examples of the use of telegraph and railways providing an impetus to the RMA, that Cohen provides are the American Civil War and the War for German Unification. In both the American Civil war and the German war for unification, the military strategists made an excellent use of the telegraph for transmitting secret messages during war, and railways for the manoeuvring of the armies. Cohen writes, giving the instance of American Civil War-"The Union shifted 25000 troops, with artillery and baggage, over 1100 miles of rail lines from Virginia to Chattanooga, Tennessee, in less than 12 days. Further, the railroad, in conjunction with the mass army, made mobilisation at the outset of war a critical element in the efficiency of a military organisation." (Cohen 1996: 37- 42).

Murray also cites the examples that Cohen has cited, however he goes a little step further to say that technology is not the sole factor that undergoes a revolution or transformation. He believes that the Industrial period, which began with the Industrial Revolution, can be said to have undergone not just one, but more than one RMAs, because the Industrial period has given not just the technology, but a whole set of changes in the organisational, political ideological, societal, conceptual, and technological changes. His opinion on RMA is that it involves putting together the complex pieces, and so the Industrial Period did not witness just the technological changes. In fact, he compares military revolutions to an earthquake, and RMAs to pre- and aftershocks. The pre- and aftershocks are restricted to one or more than one aspect (that is, technological, organisational, political, ideological, societal, conceptual), and the military revolutions are of comprehensive nature (Murray 1997). Murray gives the following two tables to show the dimensions and complexities of the Revolution in Military Affairs.

Table No. 2.1
Possible RMAs

Period	Event/ Area of change/ Product in usage	Type of RMA
14th Century	Longbow	*Cultural*
15th Century	Gunpowder	*Technological, Financial*
16th Century	Fortifications	*Architectural, Financial*
17th Century	Dutch-Swedish Tactical Reforms	*Tactical, Organizational, Cultural*
	French Military Reforms	*Tactical, Organizational, and Administrative*
17th to 18th Centuries	Naval Warfare	*Administrative, Social, Financial, Technological*
18th Century	British financial revolution	*Financial, Organizational, Conceptual*
	French Revolution	*Ideological, Social*
18th to 19th Centuries	Industrial Revolution	*Financial, Technological, Organizational, Cultural*
19th Century	American Civil War	*Ideological,Technological,Administrative, Operational*
Late 19th Century	Naval War	*Technological, Administrative, Cultural*
19th to 20th Centuries	Medical	*Technological, Organizational*
20th Century	World War I: combined arms	*Tactical, Conceptual, Technological, Scientific*
	Blitzkrieg:	*Tactical, Operational, Conceptual, Organizational*
	Carrier War	*Conceptual, Technological, Operational*
	Strategic Air War	*Technological, Conceptual, Tactical, Scientific*
	Submarine War	*Technological, Scientific, Tactical*
	Amphibious War	*Conceptual, Tactical, Operational*

	Intelligence	*Conceptual, Political, Ideological*
	Nuclear Weapons	*Technological*
	People's War	*Ideological, Political, Conceptual*

Source: *Murray, Williamson (1997), Thinking About Revolutions in Military Affairs, p.70.*

Table No. 2.2: Military Revolutions and RMAs

Pre-shock RMAs	Military Revolutions	Direct and Aftershocks
longbow, Edward Ill's strategy, gunpowder, fortress architecture	*17th Century Creation of the Modern state*	*Dutch and Swedish tactical reforms, French tactical and organizational reforms, naval revolution, Britain's financial revolution*
French military reforms (post Seven Years' War)	*French and Industrial Revolutions*	*national economic and political mobilization, Napoleonic way of war, financial and economic power based on industrialized power, technological revolution of war (railroads, rifles, and steamboats)*
Fisher Revolution (1905–14)	*World War I*	*combined arms, Blitzkrieg, strategic bombing, carrier warfare, unrestricted submarine warfare, amphibious warfare, intelligence, information warfare (1940–45), stealth*

Source: *Murray, Williamson (1997), Thinking About Revolutions in Military Affairs, p.73.*

Therefore, there occurred many military revolutions with the dawn of Industrial age. A school of thought led primarily by Toffler, that says that the evolution has not come to an end with the Industrial Age, rather the countries that have experienced the fruits of industrialisation are now undergoing the upheavals and have already entered a Post- Industrial Age . According to this school of thought the shift from industrial to information age has been aided by the revolution in information technologies (Buzan

& Herring 1998: 23). The following table shows the contrasts between the Industrial age and Information age.

Table No. 2.3

Contrasts between Industrial Age and Information Age Technology

Characteristics	**Industrial Age**	**Information Age**
Types of society	Mass – mass production, consumption, education, society, media, conscription, and destruction. World Politics dominated by a large number of similar units (states).	Fragmentation-niche (small-scale, cheap, highly specialised individualis-ed) production, etc. Nonstate actors increasingly powerful
Dominant Technologies	Hardware Stupid Machines Large Machines Oil, gasoline, diesel Standardization Quantification concreteness	Software Smart machines Tiny machines Electricity Diversification Quality and abstractness
Styles of Perception	Public perception of events as "real"	Public perception of blurring of real and fictional

Styles of organization	Secrecy Indiscriminate gathering of vast amounts of information Moderately skilled , interchangeable labour and military personnel Humans in direct economic and military control Top-down , centralized civilian and military command of organisations Stockpiling	Openness Specialised gathering of small amounts of information Highly skilled , highly specialised , hard-to-replace personnel Automation and robot control Bottom-up , bottom across organisations Just-in-time (for immediate use)
Styles of Warfare	Control of territory Maximum lethality , high casualties, little weight attached to combatant /noncombatant distinction Humans in combat Total war Mechanised war Brute force Attrition Hard Kill (physical destruction of targets) Gunpowder, high explosives , nuclear explosives	Use of Speed Minimum/ nonlethality , low casualties, strong combatant /noncombat-tant distinction Automated and robotic combat Very limited niche war Electronic war Skill Precision Soft kill (prevention of people /objects from fulfilling their purpose

		without physically destroying them Electricity

Source: *Buzan, Barry & Herring, Eric (1998), The Arms Dynamic in World Politics, p.25.*

Toffler's classification follows a compartmental and taxonomical approach that is an approach that compartmentalises the characteristics of periods. In this approach, the period of transition is almost absent by virtue of shift from one period to another. In his another work called also *The Third Wave*, the approach is to compartmentalise and contrast .He divides the history into three great waves – the Premodern or Agricultural, the modern or industrial and the Postmodern, or information. Below is given the Toffler's classification into three waves.

Table No. 2.4

Three Waves of Civilization and Warfare according to Toffler

Time Period:	**5000 B.C.**	**A.D.1700**	**A.D.2000**
Wave:	**1. (Premodern, Agricultural)**	**2 (Modern, Industrial)**	**3 (Postmodern, Information)**
Means of Wealth	Peasant-based crop production	Massified factory production	Demassified, custom information production
Central Resource	Land	Material resources	Information
Historical Milestones	Crop control Irrigation Planning and food storage	English industrial revolution (1800) American industrial revolution (1850), work mechanization, interchangeable parts Taylor scientific	Introduction of the computer Economic introduction of processing and memory Interconnection of processing and databases Extraction of knowledge from

		management (1900) —analysis Statistical process control (1945) Numerical control (1967) Computer integrated manufacturing (1987)	data Increase process understanding and precision control
Conflict Triggers	Local land ownership Clash between Rulers	Regional, geoeconomic competition Clash between peoples (states) by conscripted armies	Geoinformation competition Clash between ideologies and Economies
Core Principle of Warfare	Attrition of Infantry	Attrition of machines Mass destruction Armor and machines Hierarchy	Attrition of will and capability Precision control of perception Complex, adaptive, dispersed
Clash of Civilizations	Homogeneous conflict of powers	Bisected world (first- and second-wave states in conflict)	Trisected world (first-, second-, and third-wave states in conflict)
Military Authors	Sun Tzu	de Saxe Napoleon von Clausewitz	Sullivan Campen Libicki

Source: *Waltz, Edward (1998), Information Warfare: Principles and Operations, p.14.*

Along with this classification, Toffler also provides the cause and effect relation between the technological change and the coming of Information Age. However, this model of explaining the changes in warfare practices, despite being comprehensive to a great extent, has its own limitations. One of the drawbacks that Buzan and Herring point out is that there are still great doubts regarding even the complete arrival of the

Information Age. They write: “We are a long way from being in an information age: what we are currently experiencing is an industrial age with information age elements. There is a lot of life in the industrial age yet, and the trends are contradictory**.**” That means that the two have doubts even regarding the complete arrival of the Information Age. Secondly, the two also point out that there cannot be a complete discontinuity between the ages, because when the industrial age arrived, it did not obliterate the features of the previously existing agricultural age. After all, the new features can develop only on the basis of what already exists. So, even if the information has become a dominant factor in today’s world, it will still need industries. Thirdly, they find the classification of various parts of world as agricultural, industrial, and information based to be problematic because of presence of quite a number of agricultural societies (for instance, Somalia and Afghanistan) that are having industrial age weapons, and a agricultural society like Chiapas of Mexico, who have very intelligently used the Internet to conduct an information propaganda against their government (Buzan & Herring 1998: 24).

Therefore, there is not one opinion on whether the Information Age, which the warfare historians have much talked about, has finally arrived in a complete sense. But, the word *information* itself has come to dominate the warfare discourse. The change in the pattern of warfare practices that the computers have brought about have been seen as a part of the coming of Information Age, or the unleashing of an Information Revolution. Whatever changes are taking place in the way wars are being waged has been attributed to one big force and that has been termed *the Information and Technological Revolution,* and so there has been a rush to call the new emerging mode of warfare as Information warfare.

However, it is fallacious to say that Information based warfare solely belongs to the twenty first century, because information has been a critical element of warfare practices, even in periods when swords were used In fact, the finest example that the John Arquilla and David Ronfeldt cite is the use of information warfare by none other than the semi- literate and nomadic Mongols. He says that waging a war against Mongols was like playing the game of chess with a player who could hide the position of his pieces, but could see the disposition of both his and his enemy’s pieces Therefore; they were adept in cutting the lines of communication of their opponents.

One of their greatest campaigns was against the mighty empire of Khwarizm (which covered approximately the territory of today's Iran, Iraq, and some parts of the Central Asian republics of the former Soviet Union). What they did amounted to cutting the communication lines in order to deceive the opponent. They ensured that the correct situation was not conveyed to the Shah, by simply waylaying the messengers who were otherwise supposed to report to Shah about the position in the front. The Shah, in turn took the silence as a good sign, until one day a highly injured messenger managed to reach the capital Samarkand, only to inform that the Mongols were only one day's march away from the capital. The Shah, on hearing the news, fled in panic, and when this news spread among the frontiers, the soldiers capitulated to the Mongols without a fight (Arquilla and Ronfeldt 1996: 148-149).

It should not come as a surprising fact that the Mongol warfare strategies still are regarded as one of the finest examples of the Information campaign in the literature on warfare practices. Therefore, when the cyber warfare is defined as information warfare, then there are two consequences of doing so. Firstly, there is tendency to emphasise that only the Information and Technological Revolution has made the coming of Information war possible, overlooking so many historical instances of information warfare from the periods that had not witnessed even the Industrial Revolution. This tendency emanates from an assumption that the Industrial period has transformed into an Information Age, and so what is being called cyber warfare is actually information warfare. Secondly, what happens consequently is that cyber warfare becomes an adjunct of a broad concept called Information warfare. Is Cyber warfare really an adjunct of a bigger whole called Information Warfare? This approach (the one which sees the cyber warfare through a transformative perspective) is not without its flaws because it fails to see the details of the cyber warfare strategies which only share only some features with a very broad concept called Information warfare, which means that there are some points where Information warfare becomes a part of the cyber warfare, and some, where it is not so. This point can be clarified through a diagrammatic representation, which is shown below.

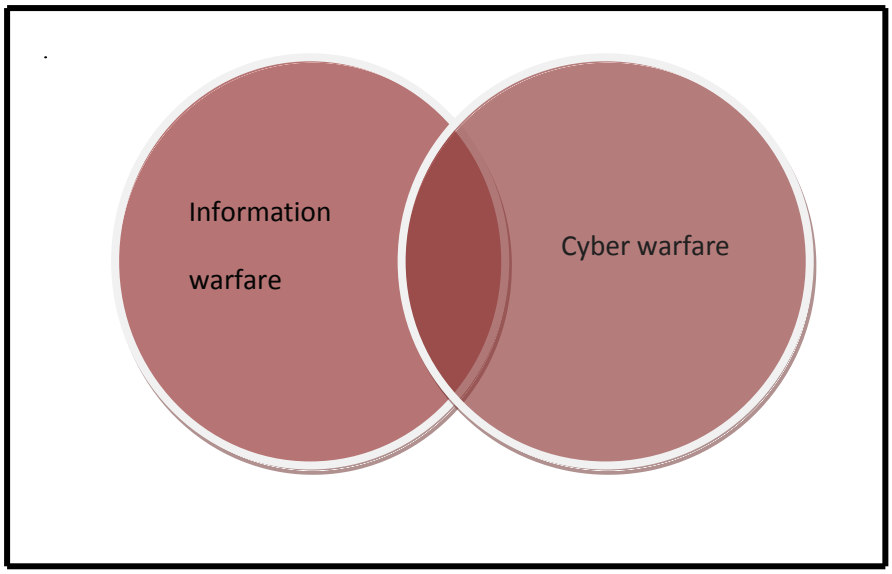


Figure No. 2.1: Intersecting Relationship

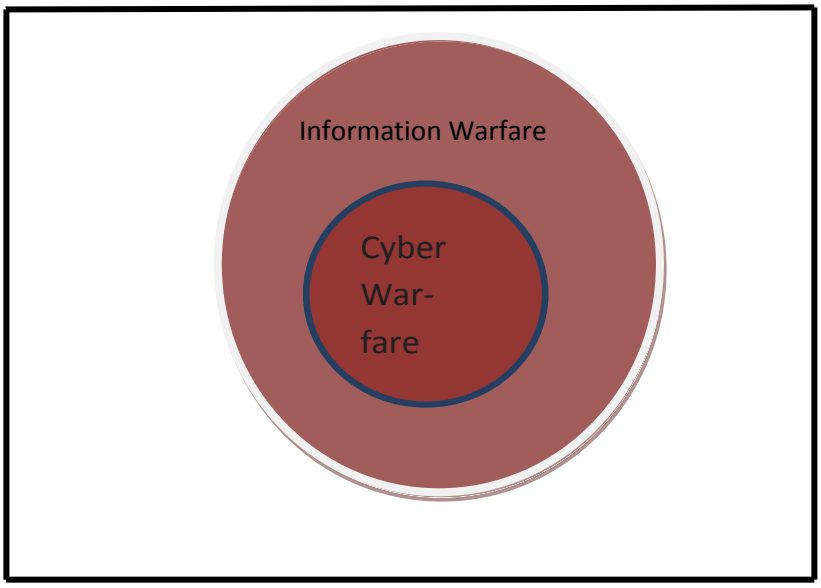


Figure No. 2.2: Subset Relationship

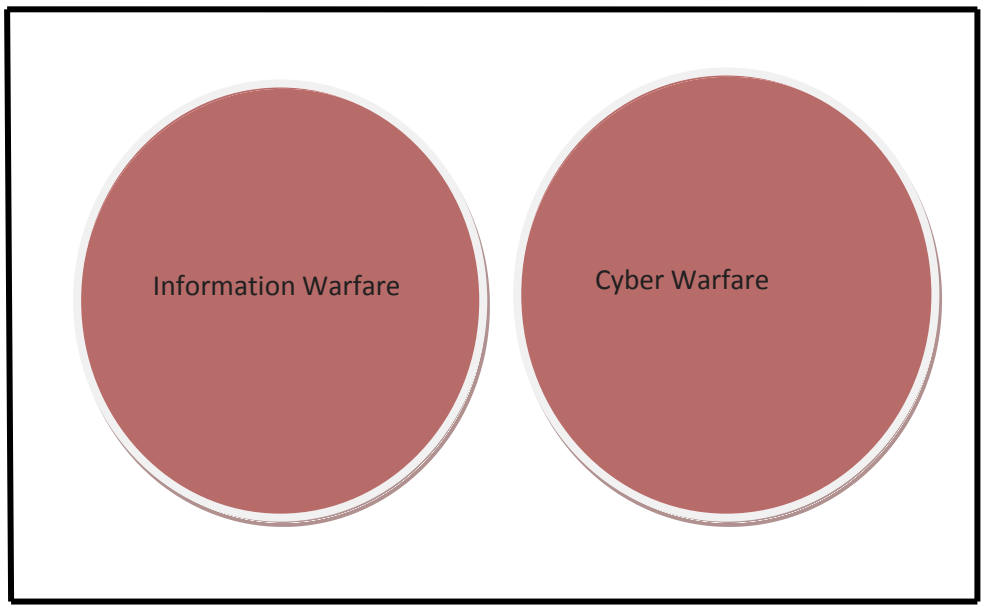


Figure No. 2.3: Disjoint Relationship

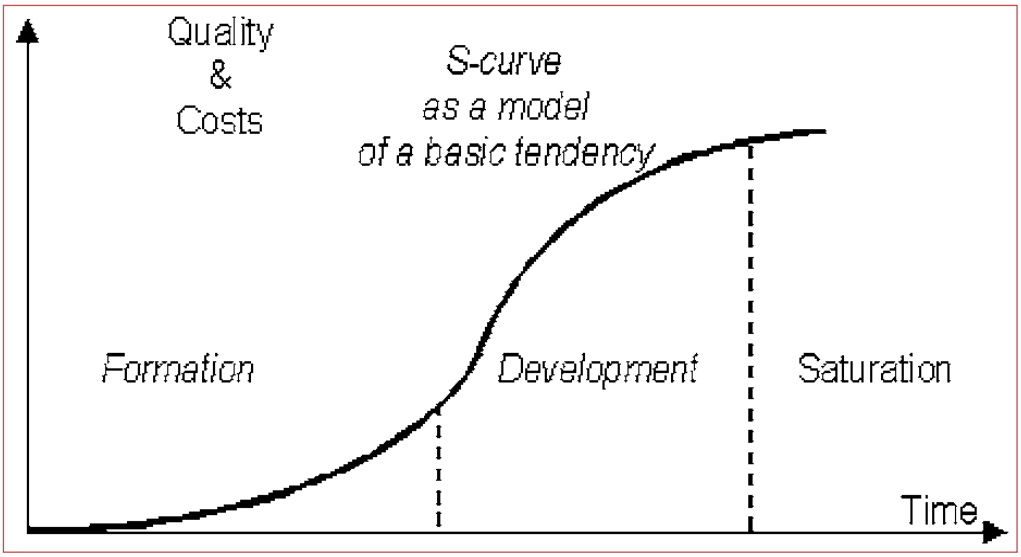
Three figures in Venn Diagrammatic form are given here, which represent basically three approaches to see the concept of Cyber warfare. The second diagram represents an approach that sees Cyber Warfare merely as a weapon of waging an Information Warfare. The diagram shows it by showing a small circle named cyber warfare in a bigger circle called Information Warfare, which indicates that despite its novelty, cyber warfare is actually a form of Information Warfare. It also indicates that cyber warfare is one of the means of waging an Information Warfare. So far, this has remained as the most popular way of defining, and analysing the concept of cyber warfare. In fact, the transformative perspective, which has been described in the preceding few paragraphs, adopts this approach only.

The first diagram represents an approach that sees only certain commonalities between the two concepts. This is the reason why the diagram shows a shaded region, indicating the points where the two intersect. Now, this is the approach which is gradually developing, but is still in a nascent stage. It gives some level of autonomy to the concept of cyber warfare. The third diagram represents an approach that shows that the two concepts are completely different from each other, and there is no

commonality between the two (indicated by two disjoint circles). So far, this approach has not received much push, primarily because the invention and widespread use of computers, and later the coming of Internet are all seen as part of Information and Technological Revolution. One can call it the most extreme approach.

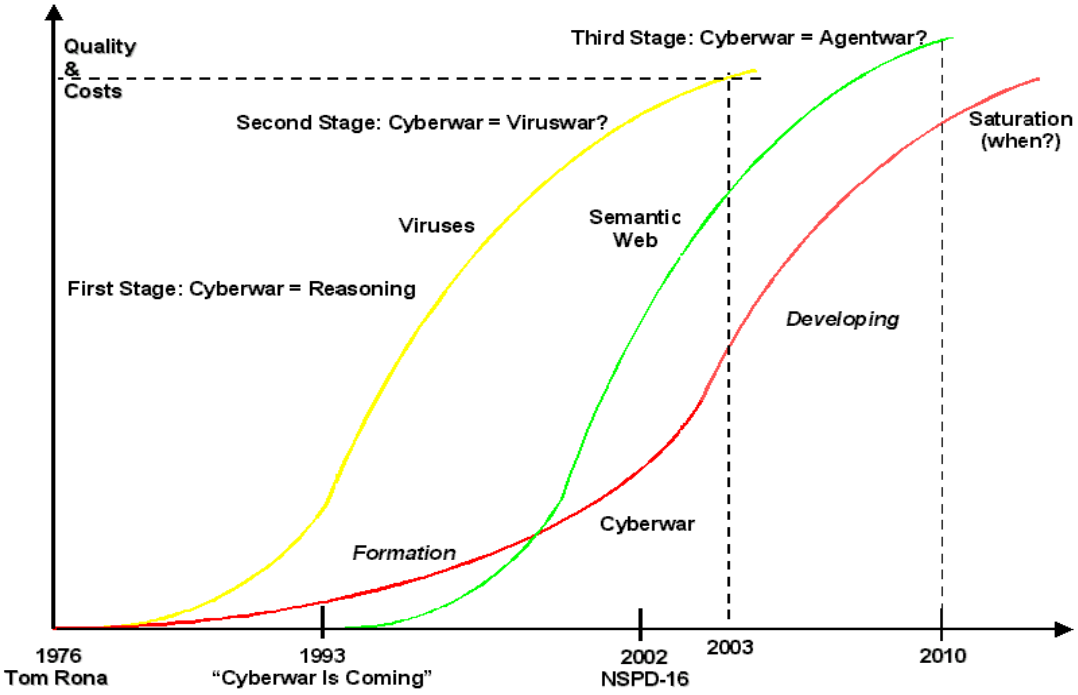
Azarov and Dadanov from Institute for Information Recording, National Academy of Sciences Kiev, Ukraine , and Arquilla and Ronfeldt explain why there has been a tendency to develop multiple approaches to understand cyber warfare. The former two, in their work titled *Instrumental Corrections for a Definition of Cyberwar* , deal with the relation between the semantics have developed in this field and multiple approaches to define cyberwarfare. What they basically do is to show a sort of development stages through an S-curve.

Figure No. 2.4: S-Curve



Source: *Azarov, Serge S. and Dodonov, Alexander G. (2006), "Instrumental Corrections for a Definition of Cyberwar", p.4.*

Figure No. 2.5: Development of Cyber Warfare



Source: *Azarov, Serge S. and Dodonov, Alexander G. (2006), "Instrumental Corrections for a Definition of Cyberwar", p.13.*

Azarov and Dadanov have attempted to show the evolution of semantics through both the curves. The first S- curve is a model curve, which means that it is a general curve which the two have modified in the second curve having three S-curves (denoted by three different colours) the first one shows one curve, which means there is basically only one factor that influence the development of S- curve, and that is time. This is not the curve that the two use to explain the evolution of the semantics in this field. It is the modified second curve that they use. In the first one the independent variable is time, while in the second one, he takes more factors- off-the-shelf technology that is already out, the developing technologies, the R&D, the intellectual factor like adversary's skills and expertise and the economic factor, one prominent being the investment on further development. Why do they take so many factors , all of which are dynamic? One primary reason is that systems do not evolve in one fashion over a period of time, rather there are dynamic factors affecting any system. So, the semantics are gradually evolving and the result is that alongside the concept of Information warfare, one is also hearing about the netwar, the cyber war. Neither the time, nor the technology has remained still in one place. It has spread, and it has

improved, making more than one S-curve possible (see second S-curve) (Azarov and Dadanov 2006)**.**

Therefore, from a perspective of semantics which Azarov and Dadanov have explained the reason for why more than one approach of looking at the cyber warfare concept exists lies in the various factors that they have listed? But, are semantics enough to explain why cyber warfare cannot have one settled approach or definition. Definitely not. Semantics are representation through words, if one simply looks at them. They tell something, but they do not tell everything, which means that the explanation given by Azarov and Dadanov if one looks from a semantic perspective is inadequate from a definitional perspective. John Arquilla and David Ronfeldt are one of those early birds who made an attempt to define and classify cyber warfares, according to their characteristics.

In 1993, Arquilla and Ronfeldt came out with their classic work *Cyber war is Coming!*, which is still widely read and referred to in various works in this field. First, it is important to explain the good points of this work, which are relevant to the queries posed here. The two authors begin with the significance of the changes that have taken place in area of Information and Technology, and call the current period the Post-Industrial period, where information is a valuable and strategic resource. True, till this point, they appear to be strict adherent of a transformative perspective that sees everything in terms of information, and to an extent they can be categorised so. But, the point where they diverge from this perspective is more important than what they make the readers see initially. And that point comes when they distinguish between the cyber war and net war, because it is in the process of distinguishing between these concepts that one is struck with both the commonality and differences between the information warfare and cyber warfare. They call netwar as a societal level conflict, which is waged with the help of military networks. It can be waged by any group, actor- state and non-state, against any kind of actor, and can be related to military and non-military issues. On the other hand, cyber warfare is an exclusively military affair, whose aim is to destroy, and disrupt the information and communication infrastructure. They call both the wars as information related (Arquilla and Ronfeldt 1996). So, according to Venn-Diagrammatic representation, their definitions fall in the second diagram (the one with the two circles intersecting).

But, the authors apply reverse gear, and term the information warfare waged by the Mongols as an early form of cyber warfare (Arquilla and Ronfeldt 1996:148-149). So, along with celebrating the novelty of this new mode of warfare, they implicitly call it an old form of warfare. Hence, the confusion that the authors had probably sought to remove is exacerbated. Broadly speaking, the confusion is what has been shown earlier through Venn diagrams. It is actually a big trap in which the literature on this field is mired. Seeking to define the cyber warfare, the literature has ended up showing what has always been there, like the information warfare. Is it not a wrong reasoning *to define something new in terms of old because it is new*? The dominant discourse which seeks to define cyber warfare in terms of Information warfare has done exactly that. The finest security analyst have woken up to the Information Warfare , *now* , when actually centuries back the Mongols had mastered the art of warfare , and the Chinese military strategist Sun Tzu had talked about war through deception . In his classical text The Art of War written in B.C., he wrote in the chapter titled 'Attack by Stratagem'- *"If you know the enemy and yourself, you need not fear the result of a hundred battles. If you know yourself, but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."* In the same chapter, he gives one of the most fundamental aspects of Information warfare, which is applied even now. He writes: *"The highest form of generalship is to baulk the enemy's plans; the next best is to prevent the junction of enemy's forces; the next in order is to attack the enemy's army in the field; and the worst policy of all is to besiege the walled cities."* (Sun Tzu 2009: 11, 13).

So, the information warfare principles were well developed in antiquity, a point which has been mentioned through another illustration earlier. Today, this point has been either forgotten or twisted. In this regard, David Londale says that a reasonable question to ask is why the existence of the information sphere, or infosphere , and the concept of information power have been noted only recently . Firstly, he not only agrees that the importance of information warfare existed even earlier, but also gives fact to substantiate it. And one of the instances that he mentions is that of SunTzu, which has been already cited. Apart from this, he gives examples from not very distant past, like the British campaign against Burma during the Second World War. At that time, Field Marshall Slim of U.K. was aware of the information support

during his campaign in Burma. He also quotes Marshall as saying, "A major difference between the Allies and Japanese during the early period of Japanese success, was that the Japanese had ample information, whereas it is no exaggeration to say that we had practically no useful or reliable information of the enemy strength, movements, or intentions." But, according to Lonsdale, the story is not same in the present times because the information age has raised our awareness of information, and the information is a tangible resource now, and many long established beliefs can be reassessed. He opines that it is true that information had significance in the past, but it was taken for granted, and time was assumed to be absolute, whereas time is now considered relative. In addition to this, there are two more reasons, and they are that the information now seeps through every aspect of human lives, and the weapons systems now rely more and more on the information systems like Global Positioning System (Lonsdale 2008: 141).

However, there is a need to read Lonsdale carefully, because he speaks from a particular perspective, and that is Revolutionary in Military Affairs. This is a familiar term by now because it was briefly mentioned in the first chapter, but in the context of 1990's. It is the 1990s that is in the mind of Lonsdale, when he talks about the infosphere. It should not be forgotten that when the Americans heralded the success of Operation Desert Storm, they called it the information warfare. Broadly, the American approach then, in the immediate years after the 1991 Gulf war was to see the Information warfare as something that involved use of information, communication technologies to make the attack more lethal and potential. An American Lieutenant Colonel Andrew F. Krepinevich, who had written an assessment of a prospective late twentieth –century developments in the military technology, argued in 1994 that:

> Revolution in Military Affairs is what occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organisational adaptation in a way that fundamentally alters the character and conduct of conflict by producing a dramatic increase –often an order of magnitude or greater –in the combat potential and military effectiveness of armed forces (Watts2011:3).

However, the Americans did not stop there. The success in 1991, stimulated their minds further, and brought to their attention to the significance of the cyberspace. The literature that was developing was best made use of by the Americans because no sooner had the twentieth century gone; US came out with its *National Strategy to Secure Cyberspace* in 2003(Kuehl2009:25). Therefore, one of the reasons for the

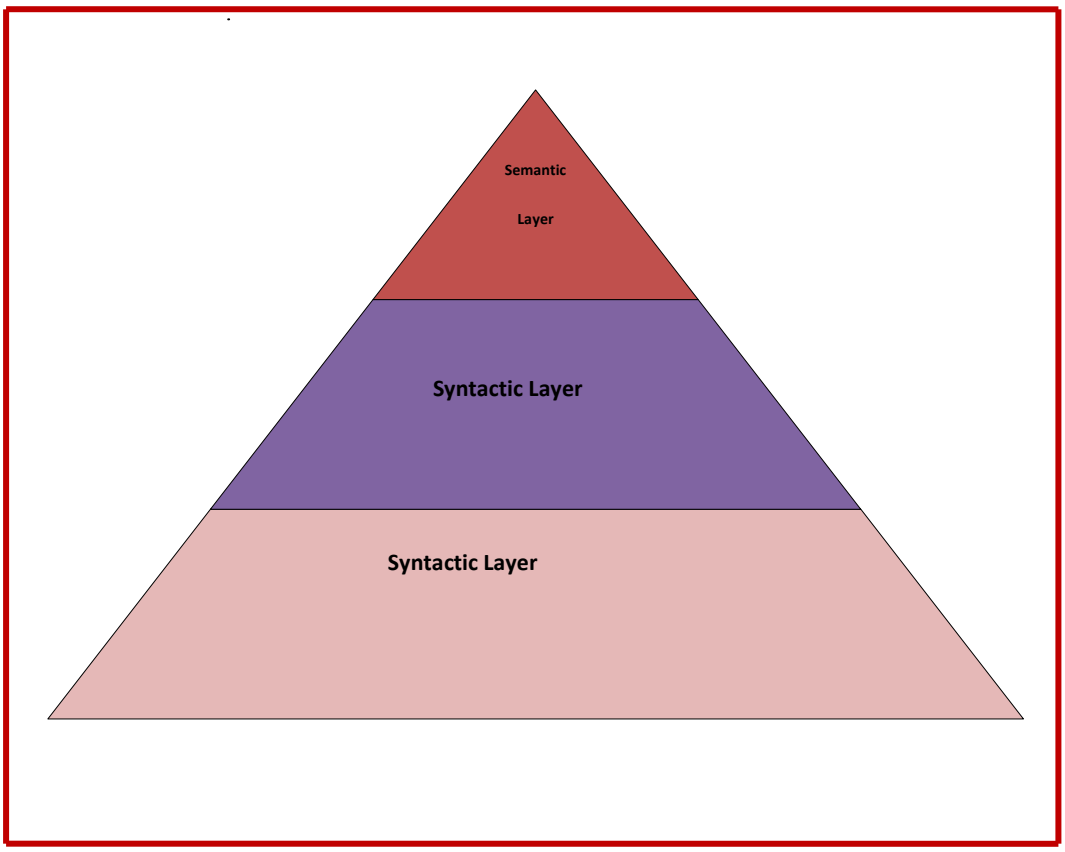
approach to cyber warfare, which has been denoted by second circle, is the push given by Americans. Does United States possess the muscles and brain to push forward its outlook and approach in the globe? It definitely has, and hence this is another reason why cyber warfare is predominantly approached from information warfare. So, when Lonsdale talks about the cyber warfare in the context of Information warfare, he is showing a similar understanding .However, gradually an approach is developing that seeks to give a conceptual autonomy to the cyber warfare. One of the representatives of this approach is Martin Libicki. He gives few points that clearly reflect this approach, and they are as follows:

- Cyberspace is a thing of contrasts: a space similar to other physical spaces like land and, water, and sea, but is also unlike these physical spaces.

- Cyberspace has to be understood on its own merit, and only then it is possible to point out what works in physical space and what does not in the cyberspace.

- Thirdly, cyberspace is a virtual space, much less tangible than land, air and water. It has three layers - physical layer, syntactic layer, and on the top semantic layer. The physical layer consists of information systems that can be destroyed, for example computers. The syntactic layer consists of basically the instructions that the users and designers have given through which machines interact with each other. And the third layer called semantic layer contains the information stored in computers. Hacking usually takes place both at syntactic and semantic levels (Libicki 2009:11-12).

Figure No. 2.6: Libicki's Three Layered Structure of Cyberspace



Perhaps, this understanding is one of the reasons why Libicki regards cyberwar as a new phenomenon that cannot be subjected to only an old understanding based on other forms of warfare, to arrive at a right picture. This clarity however was not there in the mind of Libicki more than a decade back. He had in his mind not just cyber warfare , but also many other terms that were competing in the literature for the slot- command and control warfare, intelligence based warfare , electronic warfare, psychological operations (PSYOPS), hacker-software-based attacks, information economic warfare , and cyber warfare. That was way back in 1995, when the winds of change had begun to blow, and the literature was taking baby steps (Libicki 1995**).** Libicki had in mind not only the American operations in Iraq, but also the various other kinds of scenarios. Even though he has envisaged a clearer picture, the literature still has a long way to go before it settles on one understanding.

What, however, clearly comes out of this discussion till this point is that it is not necessary to define cyber warfare in one concrete way, because the moment it is defined it excludes some crucial feature that should have been included in. The urge to define is very widespread among the community of scholars and the efforts often pay off, but in this area it is more meaningful to keep it undefined. In the first chapter, it was repeatedly mentioned at various intervals that the word cyberspace has remained undefined. It is now time to say that the word cyber war is now as amorphous a concept as the cyberspace. In one context, it is one form and in some other context, it metamorphoses itself to acquire a new. In fact, the questions such as when does something become cyber warfare, and what form does it acquire, are determined by the following factors:

(1) Is there an actor who has unleashed a cyber attack?
(2) Who is the actor (the attacker and the targeted one)?
(3) Is attacker hidden or revealed?
(4) What are the aims and objectives of the actor who first makes a cyber attack ?
(5) What are the weapons that have been employed? Or what are the modes of attack that have been employed?
(6) What are the targets of the attack- both the immediate targets and the end or the final target?

Therefore, there are basically few key words in the above five questions– *actors* (both the actor who attacks first, and the one who has been targeted, and the hidden or revealed), the *nature of targets* (the immediate and the end), and the *nature of weapons*. These three factors determine the form or the type of cyber warfare. By virtue of this, cyber warfare can be termed amorphous in nature.

Figure No. 2.7: Actors and Forms of Cyber warfare

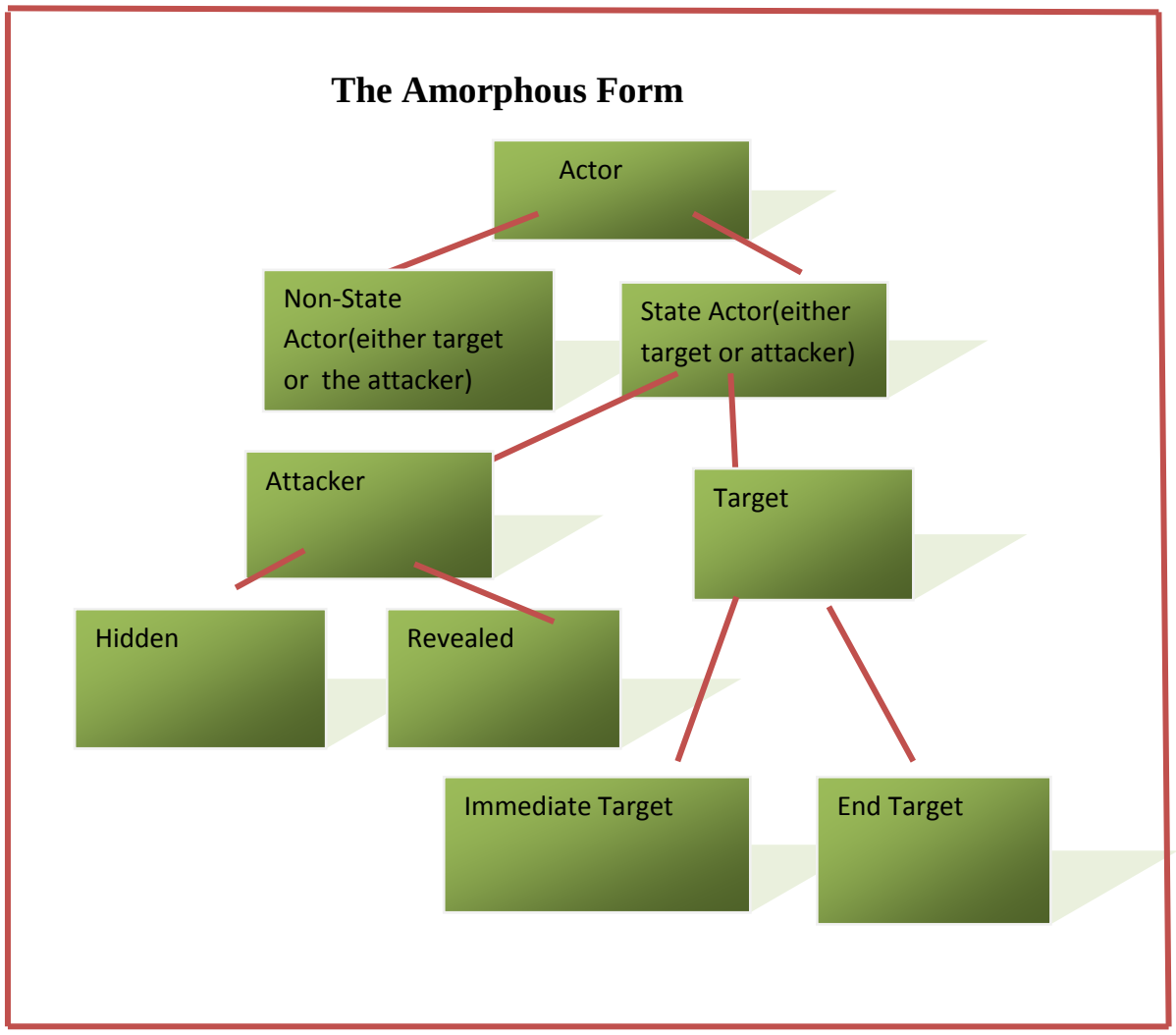


Figure: 2.7 depicts some of the situations in cyber warfare. Notice the rectangle at the top, and two diverging lines at the bottom of which there are two rectangles depicting non-state actor, and state Actor. Here, one needs to go back to the point in chapter one, where the role of state and non-state actors was mentioned. The first part depicts exactly that. In a cyber war, both the state and non-state actors can be either target or the attacker. The non- state actors could be terrorist groups, an individual hacking group, or any international organisation, groups, etc. The state actors usually refer to the intelligence organisations, military organisation, scientific establishment of a state, or any establishment that comes under state control. The attacker state actor can either remain hidden or reveal itself. Similarly, the target state actor can have immediate target, or the end target or both. This chapter takes up those cases, where both the cases are state actors. These cases will broadly reveal why certain concepts like

deterrence are not likely to work in situations of a cyberwar, and might even undergo some changes to an extent where it cannot be termed deterrence.

Case I: The Revealed Attacker

There are two state actors, and the actor who attacks is revealed, which means that on getting attacked, the target country knows who did it, and the actors outside this also know clearly who is attacking. This is possible -

- If just before the attack takes place , the two countries experience considerable friction and tensions, making the armed conflict look imminent, or,
- If there is already an armed conflict going on , or
- If a combination of two conditions is present

The above conditions are those in which the attacker is most likely to be revealed to a party other than the one which is attacked, and so here this is nomenclatured as the *Case of Revealed Attacker*. From not so distant past, there are two instances which can be put under this case. The first case is the 1991 Gulf war. In this instance, there was no element of surprise, because the tension between United States and its allies had acquired a very serious proportion when the Iraq under the Saddam Hussein regime invaded a US ally Kuwait. The conflict became just a matter of 'when' and not 'if'. Therefore, to a large extent, this instance had the presence of basically two sides –both in the nature of state actors. The first condition of armed conflict looking imminent was also present. Still, these two are not the only conditions that make the 1991 Operation Desert Storm as a case of cyber warfare. What makes it a kind of cyber warfare is the fact that in the four phased Operation Desert Storm, the , the United States had intended to destroy the command and control assets of the Iraqi forces like the air assets , airfields, in order to make the ground campaign easy. This came to be known as the Strategic Air Campaign (Putney 2004: 179-183). The emphasis then was not on pinpricking the opponent, rather making it helpless in the chaos of conflict. It is instance where the cyber warfare acquired the form of Information warfare in the first phase. Here, one cannot see the cyber warfare strategies in isolation from Information warfare strategies. Infact, John Arquilla and David Ronfeldt say that from a doctrinal aspect, cyberwar may mean defeating the enemy without completely destroying the latter (Arquilla and Ronfeldt 1993: 155). One can see that in 1991, the United States did not intend to wipe out Iraq from the

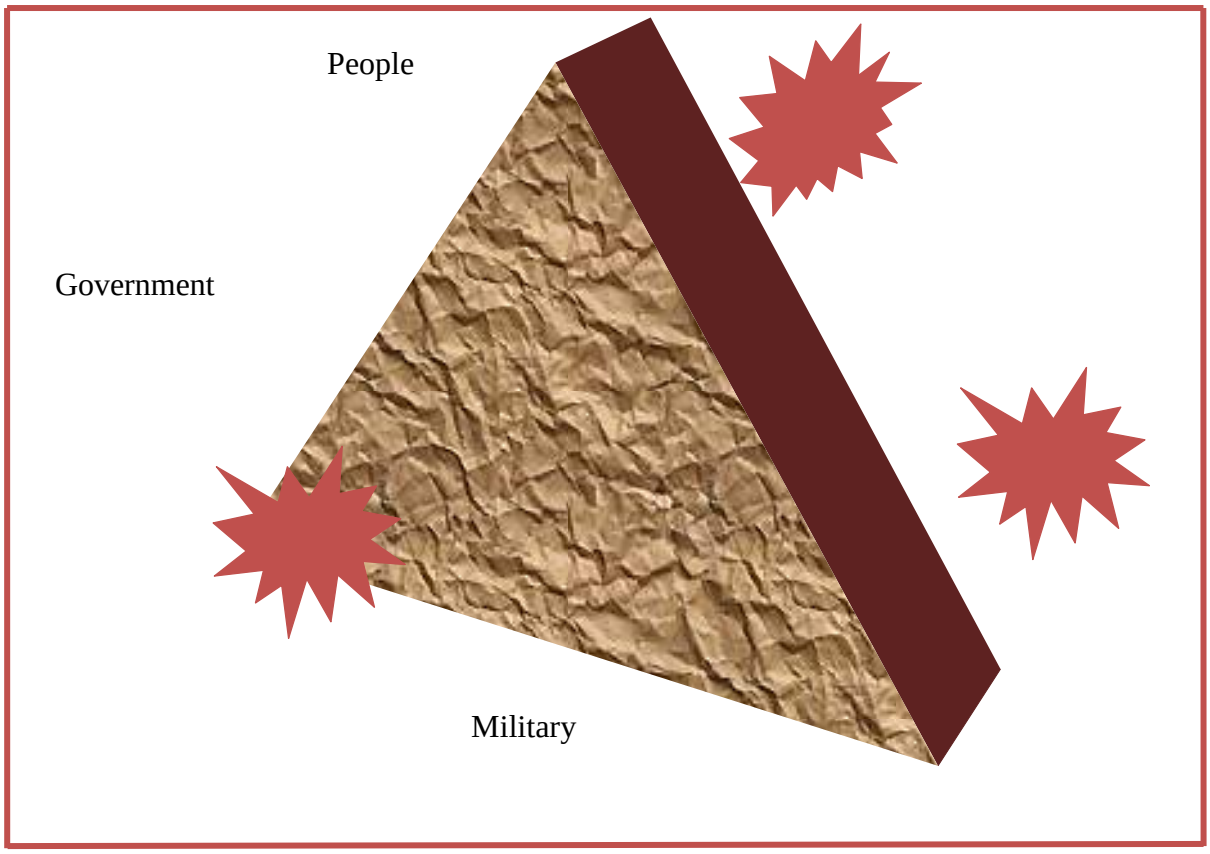
map of world. The aims were limited, rather very limited, something that caused the Information warfare, and the electronic warfare in this case to become very small. Therefore, cyber warfare was visible only in the form of doctrine, and ideas. Its physical dimensions were put into flesh only by the Information warfare. Hence, this becomes the case where the attacker is revealed, but the cyberwarfare is subsumed under the Information warfare (see the Venn Diagram, Figure: 2.2).

There is another instance, from a nearer past (from the first decade of this present century), which can be categorised under the case of revealed attacker, and that is the Russia-Georgia armed conflict in 2008. The previous instance was a simple case. This one is a more complex case even though there were two main state actors on the two opposite sides, and the condition three (that is combination of one and two) was also present. The attacker was also a revealed one, but there were more than one opinion on who made the first cyber attack. Both the parties resorted to PYOPS (Psychological Operations), and making attacks in cyberspace like targeting each other's sensitive websites, and blocking them. The leadership of both countries made sure that the opponent felt uneasy in the barrage of salvos coming from media sources, and the cyber attacks. Anatoly Tsyganok writes –"Georgia was the first one to launch an attack in cyberspace. When Tskhinvali was shelled on August 8, the majority of the South Ossetian sites were also knocked out. Later Russian media including Russia Today also came under cyber space attacks. The response followed shortly as the sites of the Georgian President, parliament, government, and foreign ministry suffered malicious attacks from 500 IP-addresses." (Tsyganok 2008). On the other hand, Timothy Thomas says: "the Cyber attacks started slowly. Weeks before the conflict a security researcher in Massachussets watched an attack against a country in cyberspace. A stream of data was directed at the Georgian sites with the message "win+love+in+Russia". On 20 July other internet experts in the U.S. said attacks against Georgia's Internet Infrastructure began at that time as DDOS attacks" **(**Thomas 2009: 56).

However, despite this confusion, it is still safe to say that in this instance, the cyber warfare strategies were not in the form of command and control warfare, that the Americans had resorted to in1991. Also, apart from the case similarity, they were similar in one more aspect, and that was that the aims of the attackers in both cases

were limited in nature. Therefore, the question arises –can the concept of deterrence have a life in this framework? Yes, but in a limited context. Amit Sharma explains how achieving deterrence is possible. The terms that are key to understanding his model are- strategy for conducting cyber warfare, and the campaign planning for strategic cyberwarfare. He explains the strategy part by relying on the Clausewitzian concept of Trinity , which consists of three forces- the people, or the will to fight in terms of manpower, finances, and support, the second element is military, and the third is government , leadership , and direction (Sharma 2009: 6).

Figure No. 2.8: Clausewitzian Trinity



Source: *Sharma, Amit (2009), "Cyber Wars: A Paradigm Shift from Means to Ends", p.9.*

The triangle given here depicts the concept of *trinity*. According to Sharma, the planning of the strategy for cyber warfare involves completely destroying the trinity so that the state as a whole fails. Here he discusses two kinds' deterences- one which he explains more implicitly. For instance, he opines that in order to deter the opponent it is essential that the all the three elements of the *trinity* are given paralytic effect. If

the attack is not strong enough, then the deterrence might fail to work. The second kind of deterrence that he talks about is included in the campaign planning, which basically involves finding vulnerable points of opponent and showing off ones cyber capabilities through minor a cyber attacks. Here, the cyber deterrence might fail if the opponent seizes the initiative and makes the attacking move (Sharma 2009: 6-10).

The model generated by Sharma, however, does take into account the fact that countries do not always have the aim of completely (morally, physically, financially, militarily, and politically) vanquishing an opponent. International politics is not likely to continue or survive if states begin to have unlimited aims of completely vanquishing each other. Moreover, even if the Trinity fails, there is something that survives, which means that the failure of Trinity cannot be equated with the failure of state as a whole. Also, the aims of state actors can be even more limited, and more subtle, than the one which is shown in the case of a revealed attacker, especially when the attacker is hidden which is actually the next case.

Case II: Case of a Hidden Attacker, the Chess Board game

Now, in this case also, there are two actors, and the attacker is hidden in the sense that when the cyber attack takes place, there is considerable amount of time involved in verifying the source of attack. It is not hidden in the sense that nobody knows who is behind the cyber offense. Rather, the attacker attacks silently, and remains mum on the issue. This is a very subtle kind of cyber warfare and the targeted entity can guess the actual aim of the attacking entity. The motive of the attacking entity may be as follows:

- To show one's own strength in the field of cyber weaponisation, so that fear is instilled in the mind of the opponent entity.
- To bring the opponent to a negotiating table over some issue (Libicki 2009: 128-129).
- To simply destroy an infrastructure of the opponent, without raising the hackles in the international arena, or without raising the spectre of war.
- To expose the vulnerabilities of the opponent, or to reduce their credibility in the international arena (Libicki 2009: 126-127, 54-55).

The third point demands some elaboration, as it is based on the assumption that the attacker assumes that no serious harm will come from the target state, even if it is easily identified by the opponent. To what extent it is actually rational on the part of the attacker is debatable, because it is equally probable that the attacker wants a pretext of open confrontation or conflict in order to financially, economically, and politically destroy the opponent. If the attacking state entity happens to be militarily, economically, and technologically less powerful than the target, then it is least likely that the attacker wants an open armed conflict. It is unthinkable that it would desire its own destruction. However, if the attacker happens to be extremely powerful, powerful enough to destroy the target, then it can be assumed that it wants an open conflict.

Figure No. 2.9: Case II Case of a Hidden Attacker

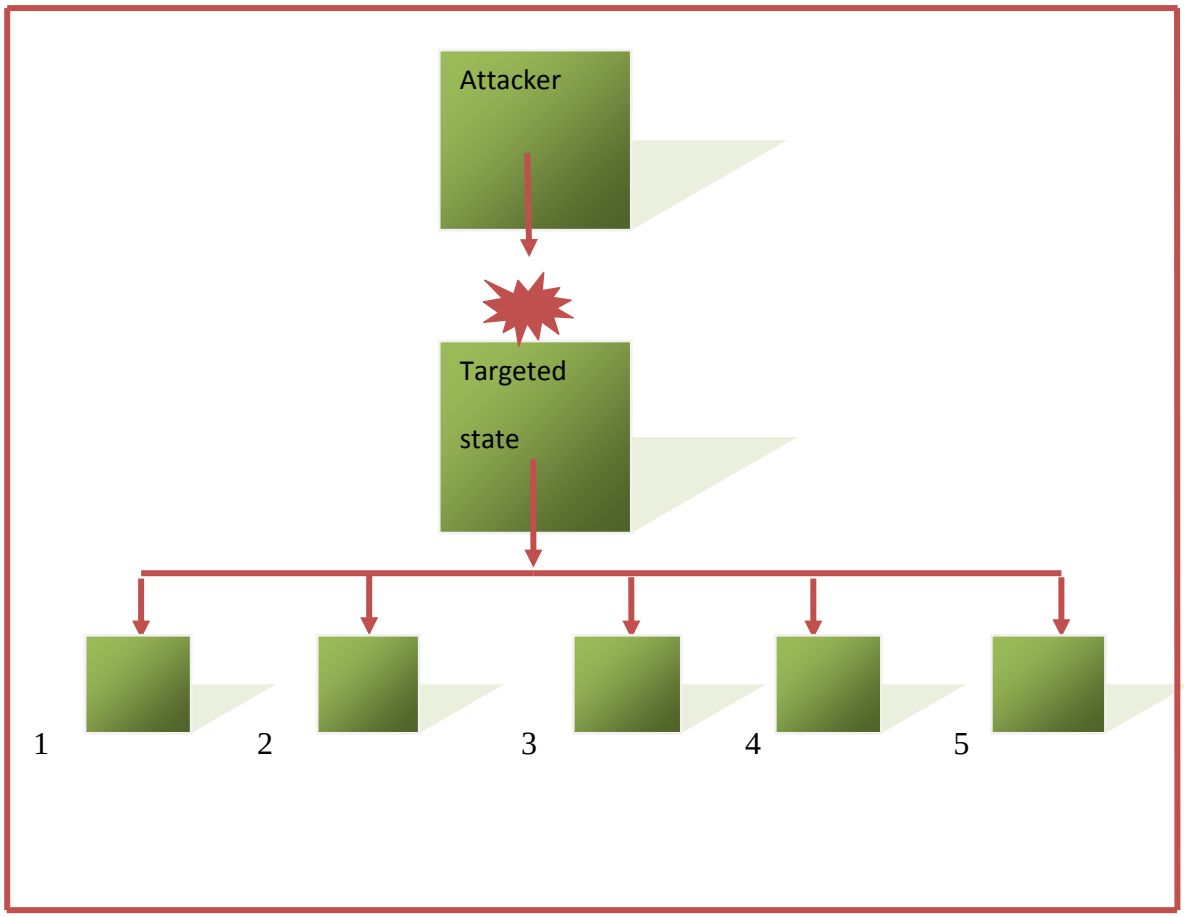


Figure: 2.9 above shows that the attacker, by attacking is actually providing stimulus to action. It tests the cognition of the targeted entity, because even though the targeted state, after the attack has many options on the table, it is very difficult to calculate

which option is really in favour of the targeted state. It is depicted in the Figure 2.9. The targeted state has five options (in this diagram). Those options could range from remaining mum to launching a retaliatory cyber attack.

In the present world, there are more instances of these cases than the first case of the revealed attacker, because as Libicki rightly points out that the ambiguity hides the reality for some time and is a major irritant to a true understanding of the situation. In fact, the Figure 2.9 depicts Libicki's view. The presence of so many options in a situation where the attacker has remained mum on the attacker, crowds the mind of the targeted country. It is a situation where the targeted country can neither afford to quickly retaliate in the physical space, nor remain completely silent. A lot in this depends on reading the mind of the adversary along with timely action. It is for this reason; this chapter chooses to call this case as the *Chess Board Game.* For the state actors, this is game that they love to play, and more so in recent times, the evidence of which is provided by none other than state actors themselves. The governments of countries in the Western world, like United Kindgom , and Germany, along with United States have been vehement in pronouncing China and Russia as two main culprits behind the cyberespionage activities going around the world . And as expected, Russia has been silent on this accusation, while China has managed to counter charge the West. So far, this has proved to be game of nerves for both the parties, and behind the veneer of peace, the countries continue to snoop and hack. One of the most talked about instance of this case is the Stuxnet. This is a type of cyber worm which was discovered in June 2010, and had struck the Iranian nuclear facility at Natanz. This worm managed to cause disruptions in the frequency of the electrical current that powers the centrifuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed (Farwell & Rohozinski 2011: 23- 25).

Now, in this case, even though it is obvious in the context of the Iranian nuclear issue that those parties that sought to restrain Iran from developing technology are the most probable culprits behind this. But it is quite difficult to pin point and blame a particular actor or a bunch of actors in the public. Also, for a country like Iran, quick retaliation to whoever it suspects cannot be an easy option, given the fact that there are powerful countries that suspect its intention behind developing civil nuclear

technology. So, the response that came from Iran was muted to some extent. It acknowledged that there had been problems with the centrifuges in the reactors, but fell short of raising a loud alarm, despite of the serious threat that the worm had posed to its nuclear plant at Natanz. However, understanding cyber attacks of this and other sorts , is difficult without knowing the nature of the cyber weapons , and cyber warfare strategies that are employed for a set purpose. So, it is now time to move on to next section that briefly discusses the nature of cyber weapons and cyber warfare strategies.

Strategies and Weapons

Hacking

The fluid nature of the cyberspace and the amorphous form of cyber warfare permit the possibility of multiple strategies and weapons. In the context of cyber warfare, hacking is a weapon, even though in some other context, it can be defined as mere activity in the cyberspace. The nature of aim determines the nature of hacking. Two illustrations will show it. First illustration deals with the espionage. Today, the urge for snooping in the cyberspace has increased among the state actors because of so many open doors through which the weapon can enter to perpetrate the attack. One of the most common ways to snoop is to hack the sensitive networks of the opponent state actor. Virus, worms, Trojan horses, Key loggers are the common tools to hack or break into computer networks. Michael Vatis writes that cyber espionage, by now is a well established activity among intelligence agencies, because as early as mid 1980s, the hacking was resorted to break into secret data. For instance, between 1986 and 1989, a ring of German hackers penetrated numerous military, scientific, and industry computers in the United States, Western Europe, and Japan, stealing passwords, and other information that they could sell to the Soviets (Vatis 2006: 59). Kevin Coleman Cyber Intelligence or Snooping basically involves digital trespassing on foreign governments and the computers operated by foreign governments, corporations, and individuals. In this, it is difficult to disguise the return path for information obtained from the cyber bugs that compromised computer systems, direct interaction with the intelligence collection mechanisms is risky, and so the middlemen are required. He cites the example of Storm, which is a vast botnet(that is a huge network of infected computers , called zombies that are linked by the Storm worm (Coleman 2008: 4).

However, the same types of cyber weapons (that is worm, virus, and other malwares) can prove to be more lethal, and more offensive in nature, and can shock the adversary to an extent where there can be confusion for some time. The next section discusses it.

Targeting SCADA (Supervisory Control and Data Acquisition)

SCADA systems are designed for real time data collection, control, and monitoring of critical infrastructure, including power plants, or other applications requiring computer –controlled equipment. This relies on the PLCs (Programmable Logic Controllers) that is computer hardware to control a physical component. In order to program the PLC, the administrator connects it to a standard Windows computer, and is unplugged when it is ready for use. For instance, if centrifuges are to be run, the administrator connects the PLC to a Windows computer, and runs a program for giving instructions to run. But if the computer that is connected to PLC is infected with a worm like Stuxnet , then Stuxnet intercepts the instructions , and sends its own instructions , but the software reports back to the Windows that correct instructions have been downloaded (Shakarian 2011: 2)**.** According to results of Project Grey Goose, SCADA systems are really vulnerable to the worms, and malwares, primarily because the dangerous malwares can cause serious disasters and accidents (Carr 2010).

Therefore, the use of worms, viruses and malwares are not confined to snooping activities. They can be more lethal weapons, if they succeed in blowing up a network of infrastructure. And the same set of weapons, when put to still different use can be weapons of PSYOPS. For instance, Storm(which has already been cited in context of cyber snooping or espionage) can generate more instructions per second than even the fastest supercomputers is not only growing, but has also got the potential to launch a massive DDOS (Distributed Denial of Services) (Coleman 2008: 4)**.** DDOS attacks basically make a computer or network resource unavailable to is intended users, which puts psychological stress on the people and the government due to sudden disruption. As opposed to this, the cyber warfare strategies acquire another dimension in which the strategy seeks to destroy the information and communication assets of the adversary, and so the nature of support systems and weapons also undergo change. Here, the war is open, and what one needs is the Intelligence, surveillance and

reconnaissance systems, along with silent weapons like worms, malwares, and botnets. Therefore, the cyber weapons have a huge field of operation, and what they do depends on what they are aimed at. A cyber weapon can be weapon of PSYOPS or a weapon of physical destruction as well. But, the most unique property of cyber weapons, which is unlike that of other weapons is that they have a life of their own in the cyber system, and have capability to propagate themselves in some instances. To what extent they are capable of deterring the adversary is still debatable, and so the next section that follows it logically is the one on deterrence.

Deterrence within the context of Cyber Warfare

Deterrence within the context of cyberwar is like a cracker which might or might not work, which means that it is uncertain. In fact, one can say that to a great extent, cyber warfare defies the very logic of nuclear deterrence. The first reason is cyber attack has a probability of not being even recognised as a use of force that can annihilate the adversary, far from being recognised as a use of a lethal weapon of the magnitude of nuclear attack that can inflict unacceptable damage to a target. Suppose there is a lethal virus that blows up the grid of power plants of the other one, as a result of which there is loss of lives and property. Then, can one be sure that the attacked country regards it as a use of force of the magnitude of nuclear weapons? One cannot be, because it depends upon the communication of the country that has been attacked to the attacker. If the attacked country regards it as as unacceptable as a nuclear attack , and inflicts a deadly blow to the originator of attack, then one can say that deterrence can applies because in this case the first attack and the retaliatory attack , both are likely to be of very huge magnitude.

However, if the first attack happens to be of moderate magnitude, then it is likely that the attacked country will retaliate moderately (if it is assumed that the retaliation for a moderate attack will be moderate only and not wholly destructive). Therefore, there is a question mark over whether it has the potential to be recognised as deadly and destructive.

Secondly, there are other critical questions that make deterrence problematic in the context of cyber war. Libicki takes up a case of sub-rosa cyber war, and brings out problematic points, both when the country has to retaliate. He puts up the following

questions that have answers that exist only in probabilities. They are three main questions- Do we know who did it? , Can we hold their assets at risk? Can we do so repeatedly? Apart from these three main questions, Libicki asks ancillary questions – If retaliation does not deter, can it at least disarm? Will third parties join the fight? Does retaliation send the right message to one's own side? Does one have a threshold for response? Can we avoid escalation? What if the initial attacker has very little worth hitting? (Libicki 2009: 39).

Each of these questions has answers only in probabilities, which is the main reason for the deterrence becoming problematic. Firstly, it is difficult to attribute a cyber attack to a country. The cyber weapon that has been used may or may not leave an imprint of its DNA, but a clear laying of blame on a country is still a difficult task. Secondly, in cyber war , it is difficult to model the extent of damage that a retaliation will do to the original attacker , which is why Libicki has framed this problem in the form of a question-Can we hold their assets at risk? Thirdly there are always doubts about of the intensities of one's own successive retaliatory attacks. If attacks are not of equal strength, then the retaliation might be ineffective, which is why the question 'Can we do so repeatedly?' The ancillary questions that Libicki raises are even more important because the complexities of cyber warfare come out more clearly in these than in any other situation. For instance, the question 'If retaliation does not deter, can it disarm?' discusses how it is nearly impossible to disarm the enemy, especially if the weapon is a botnet. Apart from this, if the third parties join the enemy in the cyber war, then the situation might become more confusing, and the attribution of attacks to a particular actor will become more difficult. Similarly, there is no fixed threshold limit for the retaliatory strike, and there are risks of the enemy bringing the war to nuclear realm. Finally, if the original attacker happens to be an insignificant actor in terms of power, and does not have anything worth hitting, then retaliation will be a futile (Libicki 2009: 41-70).

Therefore, deterrence in the cyber war is an uncertain affair. But, the question arise- why should the concept of deterrence even be considered in the realm of cyberspace. In a realm, where things are part physical and part virtual, and the weapons have a force and life of their own, the concept of deterrence actually dies a silent death. So, cyber deterrence is not just problematic as Libicki feels, but the idea of deterrence is

logically antithetical to the cyber warfare. Cyber warfare has its strength in the fluidity of cyber space, while a warfare based on nuclear strikes has as one of its basis the clarity of an enemy. To cite one instance is that of cyber snooping. Cyber snooping or espionage is also a subtle way of warfare , but will it be logical to talk about deterrence in this context because the original attacker can have only a very limited goal of keeping a watch on adversary. Hence, Cyber deterrence is a concept that reflects the tendency to understand this new mode of warfare on the basis of a pre-existing knowledge. The need however is to transcend this old understanding.

Conclusion

One of the old understandings that humanity is well equipped with to understand a new kind of warfare like cyber warfare is the understanding developed over a period of time on the Information warfare. According to some, this understanding has come about with the dawn of what has been popularly called the Information Technology Revolution, because this revolution has awakened the mind of the humanity to the significance of the Information in various facets of life, including in the battlefield. While, according to some other set of scholars, Information warfare is not a phenomenon of this current period, rather it formed the backbone of the warfare practices in the past as well. Both the stances cannot be set aside completely, because even though it is true that the technologies in the field of Information have undergone massive change, more so in the last decade of the twenty first century, information was fundamental to warfare practices even in antiquity.

The concept of cyber warfare has been caught in this discourse that revolving around Information warfare , which has occurred spontaneously – first the 1991 war was heralded as the point of Dawn of Information Warfare , due to heavy use of air campaign to destroy and paralyse the information , communication ,and command systems of the adversary(in this case it was Iraq). It was called C3 warfare (that is, command, control, and communication). For one whole decade, this term along with Information warfare became the point of discussions, and in security and military circles, the RMA and Information warfare turned into a *la mode.* From that period onwards, the cyber warfare has been subsumed in the umbrella of Information warfare, which has managed to explain certain things, but have bypassed a crucial point, and that is that even though the emergence of Cyberspace has happened as a

result of some technological revolutions, the former itself has acquired the power exercising control over both mind and matter. Its physicality and virtuality is mind boggling, and not as simple as a digitised information that is saved and flows information channels.

This means that even though the cyberspace lies in the information sphere, it is a force in itself, and possesses its own logic of functioning. The Information warfare approach is not an incorrect, rather an inadequate approach to explain the facets of cyber warfare. It is inadequate due to its intransigence in giving autonomy to this new kind of warfare. However, it is not the entire literature that is completely adhering to this approach. Gradually, new offshoots have grown that make an attempt to study cyber warfare from a different perspective.

Chapter 3

This chapter attempts to analyse the context in which the Russians have developed their approach towards cyber warfare. By context, one refers to the period, situation, and circumstances. This chapter goes about this by dividing the discussion into two contexts - the Soviet Context, and the Post-Soviet context. The Post-Soviet Russian Federation is still young by virtue of the fact that its birth has taken place in the not so distant past. Therefore, a large part of technological development has taken place in the Soviet period, which forms a backdrop for the development of Russia's cyber warfare strategies in the Post-Soviet period.

The Soviet Context

By the term Soviet context, one does not mean the whole umbrella context, beginning from birth of Soviet Union. What is significant from the perspective of the cyber warfare is the politico-scientific context of the times during the period of Cold War. Roughly, this context began to develop its clear contours soon after the Second World War was concluded. The dropping of atomic bombs in Japan by United States was one of those events that enabled this politico-scientific context to develop harder and more definite contours. Basically, this context was the intertwining of scientific developments with the power politics in a way where scientific development became one of the most essential ways to project the power of the state, and the coming of atomic bomb was to only strengthen it further. In other words, it was the politics that took up the reins of science in various areas, and gave birth to the politico-military objectives of science. That meant that the two major powers during this time were not satisfied with just the academic research in the fields like physics, chemistry and life sciences, and information technology.

In fact, according to Kojevnikov, the direction of research in the field of physics took a sharp and definite turn after the 1945. He opines that this change can be discerned if one sees the science and technological development in Soviet Union during Stalin's time, in phases, and so he sees the development in phases, each having a characteristic feature. In the first phase (pre-1941), the research was geared towards the academics,

in the second phase (1943-45), the research was in small scale, it included classified laboratory investigations, and the third phase of Stalin's reign saw an all out military industrial effort. The Soviet intelligence sources had already gathered enough information about the Manhattan Project[19] in United States to expect some change, but the way the war was concluded by United States, brought a sense of urgency in Soviet Union. Stalin ordered that everything should be directed towards achieving that most coveted bomb within the shortest possible time, so much so that in a public speech, he gave a slogan *"Dognat' i peregnat'!"* ("To catch up and to surpass!") (Kojevnikov 2004: 126-157).

So, each and every achievement of the other camp had to be responded at the earnest by showing lavishly the superiority in the same or in the other field. Science turned into a pawn of power politics game, which sought to create a sense of urgency in the opponent's camp. So, if there came an atomic bomb on one side, the other side lost its sleep but made sure that they too had it very soon. Even the innocent looking Internet which has today become a symbol of globalisation and blurring boundaries between countries and people had its origin in such a context. It began as ARPANET, which can be termed as the mother of the Internet. The launch of Sputnik in 1957 had been done to redress the power imbalance that the Soviets had perceived then (Brzezihshi 2007: 24-26). According to Michael Banks, ARPANET had its beginning in the year 1957 when the Soviet Sputnik was launched. The launch of the Soviet satellite again created that sense of urgency in the American camp, and there developed an attitude that something had to be done to give a fitting response to the spectacular jump in the Soviet science. Dwight D. Eisenhower, the then President of United States made sure that the areas of rocketry, electronics, and atomic power were given impetus. As a result, the government backed research projects in these areas grew fast. Eisenhower called the best brains to work to meet the challenge in these fields, and the result was the birth of ARPANET (Banks 2008: 2). The table given below describes chronologically the evolution from ARPANET to Internet.

[19] Manhattan Project was the atomic weaponisation project of U.S.A.

Table No. 3.1: Chronology of events leading to growth of Internet

Year	Event/s
1958	On 7th February, 1958, Advanced Research Projects Agency created by the Department of Defence directive no.5105.41 and Public Law 85-325. ARPA's mandate was to promote and underwrite research in all disciplines and to foster technological advancement on all fronts that might be of use to field of defense.
1962	A scholar named Leonard Kleinrock presented a paper on the idea of organising and transmitting data in fixed length blocks for accuracy, control and reliability. In his Phd. Thesis also he had addressed routing, distributed control and message packetisation , a few things that are part of today's Internet. During the same period, in the same institution, i.e., MIT, there was another person called J.C.R. Licklider, a psychologist, who while working on the military's use of computing technology, conceived a notion of Galactic Network. He saw Galactic Network as a worldwide network of computers through which people could interact and share information.
1965	A person called Sutherland (also connected with MIT) gave an ARPA contract to two persons called Larry Roberts(Kleinrock's colleague), and Thomas Marill(a protégé of Licklider) at System's Development Corporation. The aim of the project was to get two computers to communicate **.**
1966	Larry Roberts along with Marill writes a proposal for a network of time sharing computers .
1968	Larry Roberts writes a plan for building a network in ARPA that would permit researchers to log in to one another's computers to gain access to data in such computers. By the middle of same year a company called Bolt, Beranek and Newman Corporation(BBN Corp.) won the contract for the proposed project. During this time Kleinrock was the head of Network Measurement Centre at the University of California in Los Angeles (UCLA). Due to Kleinrock's contribution to research in the field of packet switching technology and also because of facilities available at UCLA, the Network Measurement Centre was chosen as the first node for the proposed network
1969	BBN Corporation had contracted to build a Internet Message Processor (IMP). An IMP was made as a mini-computer, whose task was to receive the packets of data, reassemble them and send them to the host computer. On 29th October, 1969, two computers at Stanford and UCLA were connected for the first time. The message supposed to be sent was "login" but it was truncated to "lo" by a system crash. However, the system was recovered, and soon the UCLA's IMP and Stanford's IMP were communicating with each. By the end of same year, two more universities were connected with each other.

1971	Ray Tomlinson develops E-mail , and uses the symbol "@" for that purpose. In the same year Michael Hart launches Project Gutenberg. This project succeeds in providing lots of material like document and books in electronic form. In other words, the beginning of concept of e-books can be traced to this project.
1973	ARPANET makes its first Trans-Atlantic connection with the University of London, and the frequency of use of e-mail in ARPANET is recorded as forming the bulk of activities in ARPANET
1974	This year saw a major breakthrough in the coming of TCP/IP(Transmission Control Protocol/Internet Protocol). A communication protocol is basically a digital messaging format and the rules for exchanging them. In other words, it is a set of procedures to be followed for communicating that include a particular format for packaging the messages . Each message carries a particular meaning and evokes a fixed response. This breakthrough came when a proposal came forward to link ARPA like networks into an inter-network that will not be subject to a centralised control and will work according to TCP.
1977	Modems that had developed by Dennis Hayes were sold to computer hobbyists. A modem is meant for encoding and decoding the digital messages in order to facilitate the transmission of information
1978	A person called Gary Thuerk sends unsolicited commercial e-mails to 600 users of ARPANET. This marks the beginning of use of e-mails for marketing and advertisements, and later these kinds of e-mails were termed as spams.
1979	MUD (Multi User Dungeon) is born. MUD is a virtual, text-based, role playing, interactive game that is based on fiction and involves online chat. So, this can be termed as the precursor of today's Virtual World which is also based on similar principles.
1979	USENET comes into picture. It allows people to post public messages and to converse with each other around the globe. In other words , Internet-based discussions start
1983	ARPANET switches over to TCP/IP system. Later this switching over resulted in the phenomenal growth in the number of users of ARPANET.
1984	Domain Name System (DNS) created. Earlier, the Internet Protocol addresses that were numerical were very difficult to remember. The DNS makes it possible for the first time to type names that are easy to remember, and are not numerical.
1986	A point had come where every major stakeholder in the world desired a creation of a global computer network, but everyone disagreed on the question of 'how' because each stakeholder had its own horse to run in the race. Europe had Open System Interconnection as its own protocol system. This system was backed by the major telecommunication

	monopolies of Europe, and most governments. IBM had System Network Architecture (SNA), and DEC had Digital Equipment Corporation Network (DECNET) as their respective protocols. United States, at that time had ARPANET Protocol. In the 1986, ultimately ARPANET Protocol emerged victorious in the Protocol wars which had begun in the early 1980s over the choice of a global communication protocol.
1989	Tim Berners-Lee writes proposal for creation of World Wide Web, that is hypertext retrieval system, in order to make global access to vast amount of information possible. Hypertext is a text that displays the links to other texts, which can be accessed from the text that is being displayed on the screen. So, World Wide Web is a collection of texts given in web pages that are linked by links or hyperlinks (the prefix 'hyper' means 'this and beyond'). The web pages can be accessed with the help of web servers and web browsers(for example:Internet Explorer, Google Chrome, Firefox)
1991	World's first web page was created. The web page was about World Wide Web only.
1993	Both United States and United Nations came online , thereby beginning the trend of .gov and .org domain names
2001	Wikipedia is launched paving the way for collective web content generation
2004	Facebook is launched and it is opened to college students.
2006	Twitter is launched.

Source: *Michael Banks (2008), p.1-6, Cameron Chapman (2009), Roger Scantlebury (2011).*

The long table listing out some of the significant events from the point of conception of ARPANET to its evolution into Internet , and its recent decentralised version , has enough to indicate that it was the politico scientific discourse of those early years of that provided the enough cells for a whole body of cyber warfare to emerge. The question then arises- what was the scene in the Soviet computer sciences, and was it also driven by politico-military ambitions, and was it similar to that Americans? Today, Internet has become so ubiquitous that one wonders what the Soviets were doing when the Americans had launched the ARPANET in a low key manner. Given, the fact that Russians during Soviet period had developed a reputation in the field of

physical sciences, Soviet Union could not have blatantly ignored a field as useful as the field of computing. In fact, the Soviets had done lot of work by the time the Second World War had been concluded.

Therefore it is important to briefly discuss some of the points that are important from the point of view of Soviet/ Russia's participation in cyber warfare. It is not possible to discuss the whole history of computing in Soviet Union/ Russia here, as that would entail writing perhaps volumes. Moreover, for this chapter, it is more important to focus on certain points than to give a very rough, complete overview of the history of computing in Soviet Union/Russia. Therefore, the first point that comes here is the question whether the Soviet computing had a strong basis to start with. The answer here is yes, because the Soviets had not only a basis of computing, but also very strong fundamentals to begin with. According to Apokin, the development of Soviet computing industry really began in the most difficult period of the Post war years, when the reconstruction efforts were on and much was lying destroyed. So, in that sense, it was not a good time to start from. But, the fact is that it did start, primarily because the electronic and calculating devices were not new to the Soviets. The country was not having any dearth of the pioneers who could give a big push to the computing industry. One such pioneer was the great scientist Sergey Lebedev[20], who despite so many odds that the post war scenario had offered, gave both the spark and the fire to the new field of computing in Soviet Union. (Apokin2001: 76-80; Rabinovich 2011).

One of the reasons for the tough times of the computing industry in its initial stages was a reluctance to whole heartedly accept the principles of cybernetics[21]. There was

[20] Sergey Lebedev was born on 2nd November, 1902, in town of Nizhni Novgorod (on Middle Volga). After graduating, he began his career as a Junior Scientific Collaborator at V.I. Lenin All-Union Electrotechnical Institute, and got a Doctor of Technical Sciences. His greatest contribution to the Soviet computing industry lies in the fact that he gave the much needed push to inventions of computing devices in a period which was not very favourable due to the widespread destruction that Second World War had caused in Soviet Union. In 1949, he began a work on Small Electronic Computing Machine (MESM) in a laboratory in Feofania(near Kiev, in Ukraine), and by 1950, the MESM model was completed. MESM is a Russian abbreviation of Model Electronnoy Stchetnoy Machiny , and this was the first model of the Soviet computer. Apart from this, his another pioneering work was in giving the general purpose computer BESM-6, which became operational in 1967. During his lifetime, he got several state awards. He died in 1974.

[21] The common understanding is that Cybernetics is an interdisciplinary field that studies structure of regulatory systems. It is closely related to the information, control and systems theories.

an ideological environment that prevented the scientists to openly propagate the cybernetics principles, even though the field itself had the potential to do wonders for the country that was not short of talent and hard labour. In fact, it was regarded as dangerous to propagate something that did not enjoy the acceptance of ideology (Gerovitch 2002:1-10). Therefore; even a scientist like Lebedev who possessed excellent ideas had to declare that what they wanted to build was something that could make ideologically correct calculations. So in an environment of deep suspicion,especially towards the field of cybernetics, Lebedev managed to form a team of 12 designers and 15 technicians to work at a disused and destroyed monastery in Feofania , near Kiev (Apokin 2001: 78; PC Plus). However, once the computing industry got the foothold, it got entrenched permanently, and for the good of scientific progress in Soviet Union.

Computing and Defence in Soviet Union

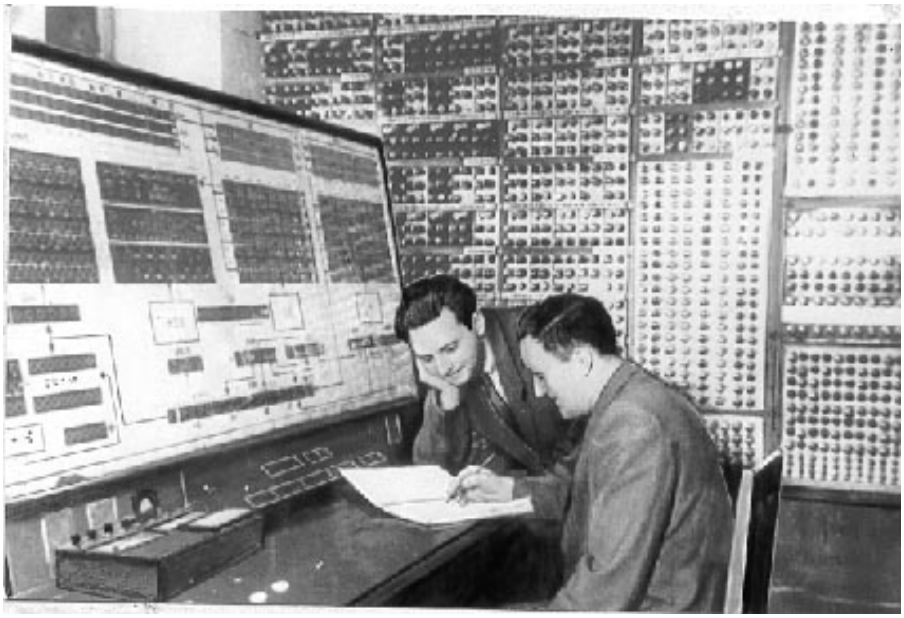
One of the most important factors behind a big push to the Soviet computing development was the defence needs of the country. As has been already mentioned, the politico-scientific context was such that the country wanted to stretch itself at any cost to equip itself with both the best brains and best machines, even if that meant resorting to pilfering of technology. In the early years of the decades of 50s , when the computing industry was only in infancy in Soviet Union, the intellectual circles of scientists was not oblivious of the defence aspect of the computer applications. In fact, to a large extent the defence needs provided the much needed urgency to the computing projects. In 1951, Lebedev at a meeting of Science Council of the ASU Institute of Electronic Technology and Heat Power Engineering said: “I must stress that the importance of work on computing machines is very high. As an example, I may present the following. The only effective way of long range rocket interception is to send anti-missile missile. To this end, we need to determine the possible point of interception. The application of calculation machines will allow for the necessary calculations for the rocket trajectory which will provide precise encounter (hit).[22]

[22] Lebedev’s words have been quoted from the minutes of the session no.1 of the Science Council of the Institute of Electronic Technology and Heat Power Engineering Ukrainian Academy of Science, held on 8 January, 1951. The document is available at the URL: http://ukrainiancomputing.org/LEBEDEV/TXT/protocol.html.

However, according to Lipayev, this link between defence needs and computing industry came only a little later, during a period that coincided with the assertion of Khrushchev after he had gained the reins of power following Stalin's death in 1953. At the outset of the 1950s, the attention was concentrated on how the computers could be made better calculating machines for solving mathematical problems. But from the latter part of 1950s onwards, the defence and military related interests started growing and now the thought turned towards how the computers could have a better data processing system and power to control military systems. This new trend in thought affected both the plants where the computers were engineered and produced and where the military equipments and weapons were produced .The demand factor here, that is the increasing demand for the types of computer that could be of great use to defence forces in controlling the weapons better, ultimately led to the diversification of computing industry. While earlier things had remained confined to a purely academic and civilian pursuit, the military demands soon changed the landscape. Firstly, there emerged a category of universal applications, which were meant for civilian uses, and then another two classes of military computers. The first category of military computers shared similarities with the category of universal ones, especially in architecture and technologies. Also, like the universal ones, they were stationary. But, the latter category was of the mobile computers. These differed both in design and systems from the stationary military computers. This kind of diversification was one of the reasons for the computing industry getting crowded with hundreds of designs of computers that were similar in functions.[23] The Table 3.2 has listed out some of the significant computer models and systems, which were developed at various points of time, for civilian and military purposes. It is not an exhaustive list, as many more models and systems were developed during the whole life of Soviet Union.

[23] See "History of Computer Engineering for Military Real Time Control Systems in the U.S.S.R." , by Vladimir Lipayev, available at Russian Virtual Computer Museum website, URL: http://www.computer-museum.ru/english/milhist.htm

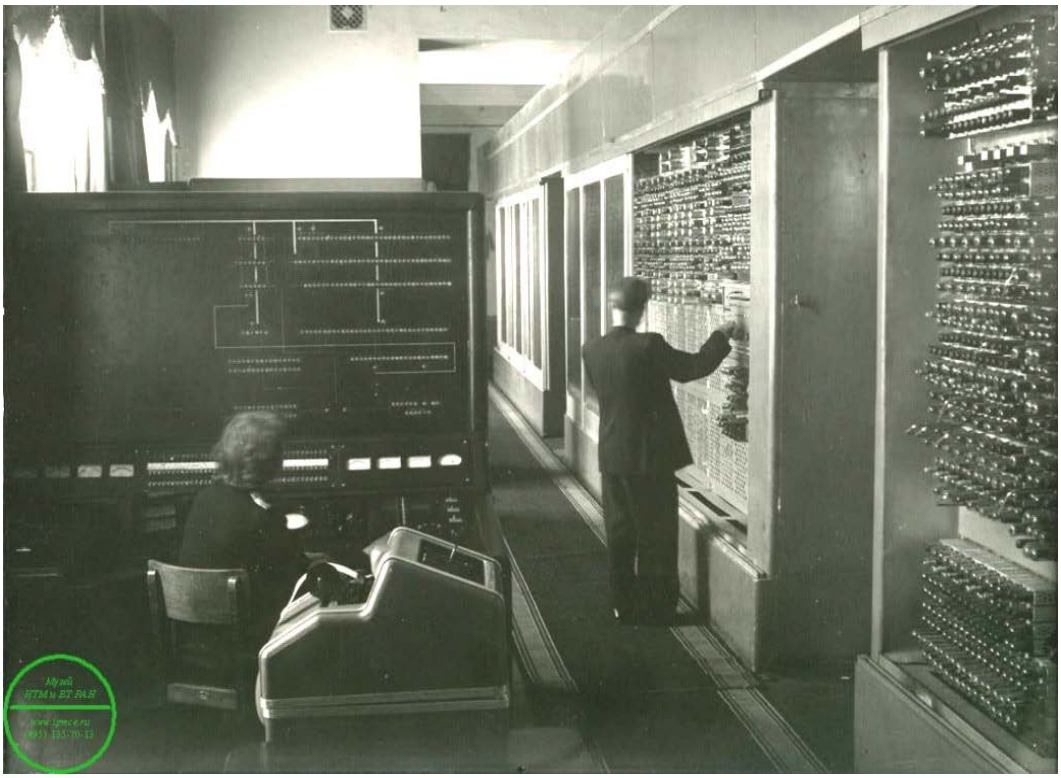
Figure No. 3.1: MESM Model of Computer



Source: *http://web.mit.edu/slava/homepage/newspeak.html*.

In this picture, two people are working on MESM, the first milestone computer of Soviet Union. They are L.N. Dashevskii(to the right), and S.N. Pogrebinskii(sitting at the control desk).

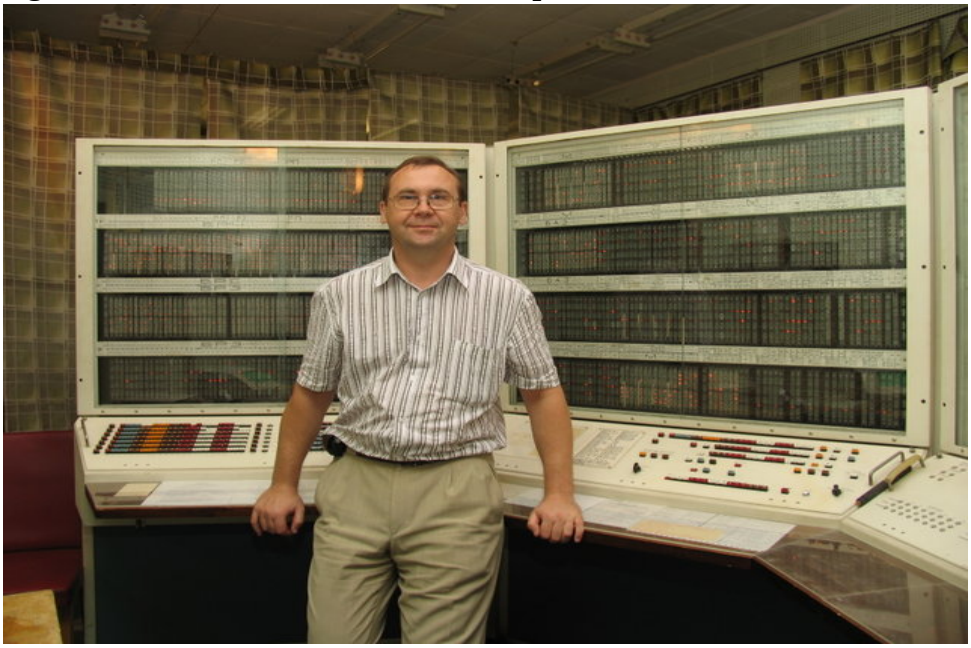
Figure No. 3.2: BESM Model of Computer



Source: *Vera B. Karpova & Leonid E. Karpov (2011), p.15.*

Shown in this photo is one of the earliest BESM models of computer, which was developed in 1950s under the leadership of Sergey Lebedev.

Figure No. 3.3: BESM-6 Model of Computer



Source: *http://en.wikipedia.org/wiki/BESM.*

This photo shows a much more advanced version of BESM. This is BESM-6.

The following table shows a small list of computing models during Soviet period, along with their applications and period of development and manufacture.

Table No. 3.2: List of Computer models and systems developed in Soviet Period

Name/Model	**Year of completion** **Of development**	**Period of manufacture**	**Application/s**
MESM	1950	Actively used only till the end of 1950s	For purposes of calculations for aiding research work in the field of computing. To an extent, it was used for calculation in rocketry and

			nuclear bomb.
BESM or BESM-1	1952		Used for tracking the path of artillery shell flight, and in the tracking the trajectory of the rocket in its space program in 1957.Also used for calculation purposes in the lab.
BESM-2	1957	Production till 1962	In computer centres, and research , for mathematical calculations
BESM-6	1967	Production till1987	For universal purposes, for scientific and engineering tasks.
M-4 Family of computers	1962	----------	Especially designed for real time control of radar systems
Radon	1964	Production terminated 1967	For anti-aircraft defense

Argon family of computers	Commercial production began in 1970	Argon-17 , the last in series went out of production in 1991	Used for controlling the spacecrafts, in the domestic airports .Argon-17 was used in the guidance system of the antiballistic missile.
5E-65 & 5E-67	Beginning of 5E-65 production in 1969, while for 5E-67 in 1975	Production of 5E-65 terminated in 1970, while that of5E-67 after the signing of SALT-1 Treaty	Anti-missile and anti-aircraft defence
A-40 & A-50	Beginning of production: A-40:1980 A-50: 1986	Still in production	For automated control of military installations
C100, C101 & C102	Beginning of production: C100: 1983 C101 & C102:1991	Still in production	For weapon control systems in MiG-29, Su-27 and Su-35 fighter aircraft

Beta-2 & Beta-3m Mobile computer systems	Beginning of production: Beta-2: 1972 Beta-3m : 1980	Termination of production: Beta-2: 1975 Beta-3m: 1990	For military automated control systems

Sources: *http://www.computer-museum.ru/english/0.htm, and Vera B. Karpova and Leonid E. Karpov (2011)*

The Explosion of Trans-Siberian Gas Pipeline

Till this point, the chapter has touched upon those aspects that show in one or the other ways that how the Soviets strived to achieve excellence in military technology in the field of computing. It is true therefore that one of the products of the politico-scientific context of the Cold War pushed the Soviets to develop their computing technology very fast. One of the positive results of this push factor was that the creativity of Soviets reached its peak, and resulted in creation of various models. But, this context of these times also proved to be a sort of cognitive trap for the Soviets later in the 1980s , a trap which brought not the ability to self introspect , but a disorder that made them suspect their own capabilities , and caused a mild paralysis in the Soviet military-industrial camp. This can be attributed to the downside of the politico-scientific context, which was nothing but an exaggerated illusion of losing the arms race, the technology race, and all sorts of races that could be possible during the period. This exaggerated illusion took over the minds of those who ultimately held the reins in various spheres of science and technology, especially the computing industry. Now, what was this exaggerated illusion as far as computing industry was concerned?

This exaggerated illusion was the belief that they could steal the ideas and beat the rival with ease, without any risk. Till the coming of BESM-6, as long as Lebedev was handling with great energy the Soviet Computing research and inventions, the Soviets were to a large extent, forming their own path in the field of computing industry. However, this was not to remain so later. Soon the computing industry took a different turn. The West beckoned many of them, which per se would not have not been bad, but this beckoning turned into a desire to simply copy the the West was

doing. In the 1960s, especially in later years of the decade, the IBM-360 System attracted the Soviets, and small amount of technology spying and pilfering started. In the short run, these pilfering activities brought some quick results. In 1972, Soviets came out with the copy of IBM-360, which was named ES-EVM. Other copies also emerged, like SM-4, AND SM-1420 mini-computers that were copies of DEC PDP-11/40, and DEC PDP-11/34+. By the early 1980s, the Soviet Union had also started operating some early versions of the Windows system. But, by now, the Soviets had fallen into the trap. Some of the technologies that had been allegedly stolen began to report minor malfunctioning or even huge delay in running operations. However, the shock came later. In the beginning of 1980s, the preparations for running the Trans-Siberian gas pipeline, and for that Soviet Union had already purchased some of the old models of American computers in open market. But they had failed to procure the necessary software for running them. Talks with U.S. over that did not bring the desired results, and ultimately the Soviets had to acquire the software through espionage. According to American and French intelligence sources, the U.S. was in fact waiting for that point to come, because the stolen software had been coded in such a manner as to make the valve of pipeline open and close erratically. Finally, the explosion came on June 1982. In this entire game, the French and Americans had used a mole in KGB , who was codenamed 'Farewell' , and it indeed proved to be a farewell task for the mole , for he was caught and executed in 1983 (Safire 2004; Weiss 2007).[24]

Now, to what extent this version is correct is a point of debate only, because this version has been popularised by the West, mainly the United States. The point here is not enter into this debate , but the fact that if this version is indeed accurate , or contains some truth, then this blast of 1982 indeed can be termed as the first case of cyber warfare of the Cold War period. In the second chapter, there was description of a kind of cyber warfare strategies which make the warfare *sub-rosa* in nature. This incident closely approximated the kind of warfare which is sub-rosa in nature. It is however quite mysterious as to why the Soviets chose not to make a hue and cry over it. If one does a reasoning retrospectively, treating oneself as an observer who is

[24] Also see for details "Declassified: The Secrets of Soviet Computing", given in PC Plus, dated 25-06-2009, and available at the URL: http://pcplus.techradar.com/2009/06/25/declassified-the-secrets-of-soviet-computing. PC Plus is United Kingdom's premier technology magazine.

detached , then the Soviet brush with the cyber warfare appears to be just one of the series of political and other kind of disasters and upheavals that brought about the demise of Soviet Union. However, this kind of reasoning will amount to giving short shrift to the context of the times. A more appropriate reasoning will be that now the Soviets had come across a new mode of offensive in warfare, they needed ample amount of time to understand it, but the time twisted it and much of the understanding has been done by the New Russia, which begins post 1991, and it is this understanding which forms a more important part as far as historical perspective is concerned.

The Post Soviet Context

Some of the fiascos during Soviet times have served as a sort of reminder to Russia and hangs there in front of it like a learning material written with chalks on the blackboard. During Soviet times, the Soviet went overdrive, and perhaps never even thought that there could be a war so subtle that it would force them to rethink and re-strategise, but the New Russia has made it a point to learn the lessons, and so in this period which is still going on, one has so far witnessed Russia that is using its arsenals sparingly, and only for 'pin-pricking purposes'. "No Grand Display of a Grand Design" seems to be the principle that Russia has followed in three of its main engagements in cyber warfare activities. It is therefore imperative to briefly discuss those three major engagements in the Post-Soviet period.

Operation Moonlight Maze

One cannot say that this is the one of the earliest engagements of Russia in cyber warfare activities, but since no other has been widely reported during Post Soviet period before this came into picture, so this can be given the status of one of the earliest engagements of Russian Federation with the cyber warfare activities. John Arquilla says "Cyber War is like Carl Sandburg's fog. It comes in on little cat feet[25], and it's hardly noticed. That's its greatest potential." (Arquilla 2003)[26] In year 1998, the Americans finally noticed that someone was following them on cat's feet. It was

[25] The expression "little cat feet" means to come very noiselessly

[26] John Arquilla has quoted this in one of the interviews given to the Frontline Magazine. It is available at the URL: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html

in that year that the Security experts first spotted the intrusions in the sensitive places in the Department of Defence computers. The U.S. Air Force and Army investigators traced the attacks to an Internet Service provider in Russia. Apart from Department of Defence, the other targets of intrusions were Department of Energy, NASA, military contractors, and military linked civilian universities. In October 1999, the Federal Bureau of Investigation (F.B.I.), formally testified to the Senate subcommittee about the F.B.I. investigations into the repeated intrusions, and it was the F.B.I. that gave the codename of Moonlight Maze, and not the party which has allegedly attacked. It has been indeed a maze for the investigators because even though they succeeded in tracing to Russia, they have still failed to establish conclusive evidence that it was actively orchestrated by the state actors (Joyner and Lotrionte 2001: 840, 841; Abreu 2001; Drogin 1999).

Estonia 2007

If in the Moonlight Maze case, the Russians were supposedly moving with cat's feet with an intention to just keep an eye on the opponents, then in this case it was making a pinch on the skin, which seems to be a measured and meditated response because the circumstances did not permit it to react in a very strong manner. The seeds for the cyber attacks were sown when the Estonian government and Russia locked horns over an issue. In 2006, Estonian Prime Minister Andrus Ansil claimed that in 1944, the Soviet Army had not liberated Talinn (Estonia's capital) from fascist occupation, and the Bronze Soviet Soldier Statue that had been built as a memorial for Soviet sacrifice was in fact a big symbol of Soviet occupation. He also ordered the statue to be disassembled and placed somewhere else. In 2007, Russia grew so furious that there were even suggestions of imposing sanctions on Estonia. On April 22, 2007, the large number of supporters of Bronze Statue began placing flowers at the statue. One such supportive group was 'Night Watch'. It kept an eye on the police who were intent on clearing them from the spot. However, on April 27, 2007, the police force resorted to tear gassing and there were riots, and on the same night, the Bronze Statue was secretly disassembled. This was followed by protests in front of Estonian embassy in Moscow.[27]

[27] See for further details "Time line of the events in Tallinn, Estonia", URL: http://www.infoniac.com/breaking/chronology-of-the-events-in-tallinn-estonia.html

However, what really struck Estonia were not the sanctions or strictures from the Foreign Ministry of Russian Federation, but a spate of cyber or digital attacks. As soon as the riots had subsided, it was one of the newspaper offices in Estonia that reported problem with the computers. The head of Information Technology division of Postimees reported that the paper's servers had been swamped, and the servers would be crashed. He resorted to turning off some not very important sections, but the servers kept getting swamped. Similar attacks were reported in business firms, and houses, government offices, banks, restaurants, automated teller machines. The end result was that life became paralysed in the country, and the Estonian government began to call Russia as the culprit (Davis 2009).[28] So the retort from Russia did not come along expected lines. Also, the attacks were of such nature that the blame could not be squarely put on the Government of Russia, because much of the attacks were traced to non-state actors. In this case, Russia inflicted a pinching, short termed subtle aggression on the opponent.

Russian Cyber Offensive against Georgia

The Russia-Georgia conflict in 2008 grabbed the headlines very easily, primarily due to high voltage engagement between the two especially at a time when Russia perceived that it did not have a very comfortable neighbour in Georgia, due to the dispute over the territory of South Ossetia and Abkhazia.[29] For Russia, the large ethnic Russian population is a plus point, a leverage point which it does not want to concede at any cost, but for Georgia (post Rose Revolution[30]), the disputed nature of

[28] See "Hackers Take Down the Most Wired Country in Europe", Joshua Davis, Wired Magazine:ISSUE:15.09,
URL: http://www.wired.com/politics/security/magazine/15-09/ff_estonia

[29] South Ossetia and Abkhazia are two territories situated between Russia and Georgia, which the latter to be its territories. The dispute over these territories dates back to the early days of Soviet Union. In 1921, Abkhazia was made a Soviet republic, but with ambiguous character. In 1931, Abkhazia was made an autonomous republic within the Georgian republic. But after the dissolution of Soviet Union in 1991, Abkhazia restored its 1921 status. In 1992-93, after a brief war with Georgia , Abkhazia declared its independence. Similarly, South Ossetia had already declared itself a free republic after a war with Georgia in 1991-992.

[30] Georgia, which is Russia's neighbor on its western flank , held its parliamentary elections on November 2, 2003. Some European international election observers called that elections did not meet all the criteria of fairness. Mikhail Sakaashvilli , who was in the opposition in Georgia soon claimed that he had won the elctions, and urged people to demonstrate against Eduard Shevardnadze who was President of Georgia at that time . So, when Shevardnadze attempted to open new session of Parliament on November 22, major opposition parties led by Sakaashvilli protested by bursting into the session by holding roses into their hands. This was followed by heavier protests by civilians, and forced the ouster of Shevardnadze on November 23. This has been popularly called as Rose

territories is a big irritant. It so happened that the two began to spar verbally over the territories, and Georgia went on overdrive and launched military attack on South Ossetia on 7 August 2008, with the massive shelling of town of Tskhinvali. Russia retaliated swiftly with land, air, and naval power. But the highlight of this conflict was not the land, air, and naval domain, but the cyberspace domain that saw increased activity before and during the conflict. The cyber aggression was not committed by just one side, but by both sides, in a very concerted manner, so as to time it according to the actual attack in the land, air, and naval offensive. Distributed Denial of Services attacks were served on Georgia's websites that were related to communication, finance, and foreign ministry. Sites were defaced[31], propaganda sites were attacked. There was heavy involvement of non-state actors- hacker groups, patriotic groups. There were even cases of cyber war between Georgian and Russian hacker groups. Till date, this cyber conflict has remained as the conflict in which Russia was most intensively involved (Hollis 2011: 1-5).[32]

Conclusion

The Soviet Period laid down the material conditions for the cyber warfare to emerge gradually as a reality by decade of 1980s, with the first brush with a cyber attack in 1982 in the form of the Trans-Siberian Pipeline blast. These material conditions were basically the technological development in the field of computing, and the spread of computing to both civilian and military areas. This development of computing took place only when the computing got a great push from the ruling establishment in the form of increased attention to computing related research works and its applications in military and civilian areas. However, the 1982 blast came as a shock to the Soviets. Before that it had not been envisaged by them that there would be a day when such attacks on civilian infrastructure could be possible without the help of any bomb or missile. The Soviet Union broke up in1991. So, the major part of the evolution process has taken place in the Post Soviet period, with Russia already having engaged itself with three cyber warfare cases.

Revolution. It is alleged that this revolution was heavily funded by Western countries to oust the pro-Russian Shevardnadze.

[31] Defacement means attack on a website, by changing its visual appearance. As a result of this attack, the affected website bears information other than what it intends to.

[32] "Cyberwar Case Study: Georgia 2008", Small Wars Jounal,pp-1-5,
URL: http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Chapter 4

Introduction

Some of the factors on which a method of warfare depends are- the fundamental principles of that particular mode of warfare[33], the power distribution of the groups that are engaging in conflict,[34] various approaches to understand that particular mode of warfare, and the already existing knowledge that has been accumulated from the past by the actors[35]. In case of cyber warfare also, these factors are important to understand its various forms.[36] The first two factors, that is, the fundamental principles of cyber warfare, and the power distribution of the groups that engage in it, and their ability to influence the cyber warfare, have been the most often discussed themes of the literature on cyber warfare. The discourses on Information warfare, and the emergence of concept of deterritorialised state, have in one or the other ways tried to discuss these factors in context of cyber warfare.[37] But, the rest two factors have been present in only selected contexts, and even those few contexts have not touched

[33] Every kind of warfare has some elements that define that particular kind of warfare, and without which it cannot exist either as a concept, or in practice. Therefore, fundamentals of a mode are the defining factors of that mode of warfare. In the first chapter, it was repeatedly stated that the cyber warfare has emerged as amorphous form that has yet to find its fundamentals. But, it can be said to possess a rudimentary fundamental in the form of cyberspace. The meaning of cyberspace might differ from context to context, but it cannot be denied that cyberspace is fundamental to the cyber warfare.

[34]The groups engaging in a particular mode of warfare have varying levels of capabilities that are required for engaging in that mode of warfare. For, instance, in a mode of warfare that relies on bombing through air power, the parties engaging in conflict might or might not be having equal capabilities to engage in a mode of warfare that uses air power. Therefore, power distribution here means how the parties are relatively placed in the area of a capability required to engage in a particular mode of warfare.

[35] This chapter assumes that an actor/group learns from past mistakes, and seeks to fill the lacuna that were present in its actions in the past, which means that actor is constantly learning. Therefore, the knowledge means the results of past actions. For instance, if in time period t_0 , the actor chose x_0 and got the result y_0, then for the next period the knowledge exists in the form of y_0 .

[36] The previous chapter has discussed how the cyber warfare is subject to various factors and can acquire various forms. Here, by various forms it means all the forms that have been discussed in the last chapter.

[37] A major part of the literature that has almost hijacked the discourse on the principles of the cyber warfare is the one that deals with information warfare, and this literature is not restricted by the newness of the concept of cyber warfare, because for the works dealing with the information warfare, the most handy thing for explaining the principles of this warfare is the old and familiar concept of information. This easy access to an old understanding has enabled the formulation of some fundamentals of cyber warfare. As to the second factor of power distribution among actors, the literature discusses emergence of non-state actors in cyberspace, and their power vis-à-vis the might of state actors, the asymmetric nature of cyber warfare waged by small non-state actors.

upon the relationship of an actor's/ group's choice of strategies, with the way the actor understands that mode of warfare, and with the knowledge it already possesses.

This chapter analyzes this relationship in the context of Russia, which means that the actor concerned, here, is Russian Federation which emerged post Soviet Union disintegration. The relationships that it seeks to study are the following:

(1) How has the Russian Federation understood the term cyber warfare, and how this understanding is helpful in dissecting the some of the important cyber conflicts that Russia has engaged in?
(2) What are the elements that the actor concerned here considers as supreme elements of cyber warfare strategies, and how they affect the way this actor chooses strategies?
(3) How does the pool of existing knowledge help Russia in designing cyber warfare strategies?

Cyber Warfare as understood by Russia

Russia has developed its approach to understand the term-cyber warfare, and for this it has relied on the concept of *Reflexive Control*. This is not new to the Russians for the fact that this concept is old and has already been studied since Soviet times. According to Timothy Thomas, the concept underwent some stages, which were research (from early 1960s to late 1970s), practical orientation (from late1970s to early 1990s), psychological-pedagogical (from early to mid-1990s), and psycho-social (from late 1990s onwards). Timothy further writes that for Americans, the idea of reflexive control might be unfamiliar to some extent, but for the Russians, it is an old concept that has been implemented in various cases. He credits some of the scholars of Soviet period for developing this concept, namely V.A.Lefebvre, V.E. Lepsky , G.P. Schedrovetsky, V.V. Druzhinin, M.D. Ionov, and S.Leonenko (Thomas 2004: 238- 239).

Reflexive Control: Definition and Process

Reflexive Control has been defined by Lefebvre as a process by which one enemy transmits the reasons or bases for making decisions to another(Thomas 2004:238). By this definition, this process is meant for engaging oneself with the opponent in such a way that the latter chooses the option that one wants him to choose .This is made

possible by the transmission of those signals to the opponent that will make the one's option appear as a rational and right action to the opponent. This also implies that this process relies on the calculating on the decision making of the opponent. In other words, it is a kind of process that works on the basis of *providing the appropriate knowledge* and *knowing the right knowledge*. Both the terms carry meaning in the context of Reflexive control. The term 'providing appropriate knowledge' means giving the bases to the opponent that will generate the reaction of one's desire, while for the first to be possible , it is possible to have the second term , which means possessing right knowledge about the opponent. Therefore, Reflexive Control is closely related to the psychology of the actors.

Its close association with the field of psychology makes it a cousin of another concept called Psychotronic methods. The psychotronic methods are those that seek to control the brain with the use of a substance, electromagnetic rays, picture, sound and light. This is also a field with which Russia is well acquainted because they have never ruled out the use of psychotronic weapons in situations of conflict (Thomas 1998).[38] However, Reflexive Control is more about the knowledge factors and the deception, rather than actually controlling the biology of the creature. According to Soviet military theorist S.A. Komov, Refelxive Control is a form of intellectual Information warfare which can be fought against people, forces, forces in the field, and systems. The intellectual Information warfare, may involve the following:

(a) Distraction: This is done when the enemy is supposedly preparing for the conflict. In this, the usual tactic is creating an imaginary threat against a vital point of the enemy, so that the latter is confused regarding prioritisation of the points to be defended.
(b) Overloading: This involves giving too much of information to opponent that are contradictory to each other.
(c) Paralysis: This is partly done through the first point as it also involves making the opponent believe that it has a very weak spot at a point.
(d) Exhaustion: This involves causing the opponent to carry out useless operations , which succeed in wasting the opponents energy, resources and morale.
(e) Deception: This is done by causing the enemy relocate to a wrong point

[38]For details on psychotronic weapons, see "The Mind has no Firewall" by Timothy L. Thomas(1998),*Parameters*, Spring1998, pp-84-92..

(f) Divisive Techniques: This is done by causing the opponent to act in opposition to coalition interests.

(g) Pacification: This means adopting a peaceful posture, so that enemy remains less vigilant.

(h) Deterrence: This is done by creating an impression of superiority.

(i) Provocation: Causing the enemy to do that is advantageous to one's own side.

(j) Suggestion: Offering the enemy information that affects it legally, or morally, or ideologically.

(k) Pressure: This is done by circulating a piece of information that discredits the enemy government. [39]

Therefore, the similarity between the psychotronic methods and reflex control is confined to an area where thought process of the brain is concerned. Russia has understood reflex control more as a game of mind, than as a game that involves influencing the biology of thought, and it sees this concept as drawing a rough sketch of the opponent, with a lot of emphasis on its behavioural traits. According to Russian military author on this subject, Sergei Leonenko, reflex action involves creating a model of the system containing behavioural patterns. For drawing this model, certain elements are crucial, which are as follows:

(1) A given situation

(2) An Objective of the model that is being drawn

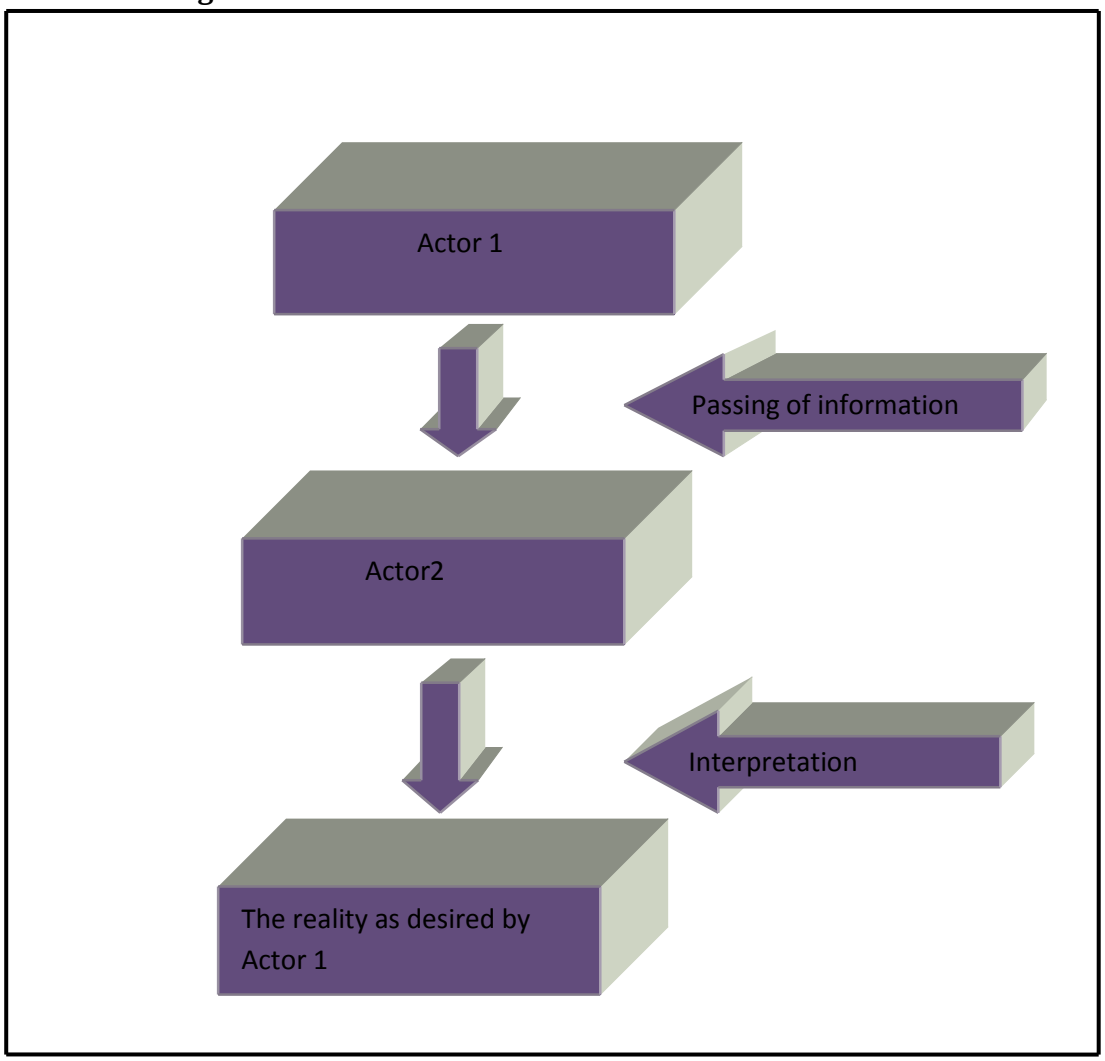
(3) Objectivity, which means that one does not have to see the model from outside. Envisaging oneself within a system is the meaning of objectivity.

(4) Moral, psychological , and other behavioural traits of the decision makers of the opponent

(5) Envisaging oneself in the place of the opponent, in order to predict what the opponent might do as a rational actor. (Thomas2009:478)

[39] For the points (a to k), see the Air University , Maxwell Air Force Base, Montgomery, Alabama, U.S.A., website. URL: http://www.au.af.mil/info-ops/perception.htm#reflexive

Figure No. 4.1: Reflexive Control in case of two actors



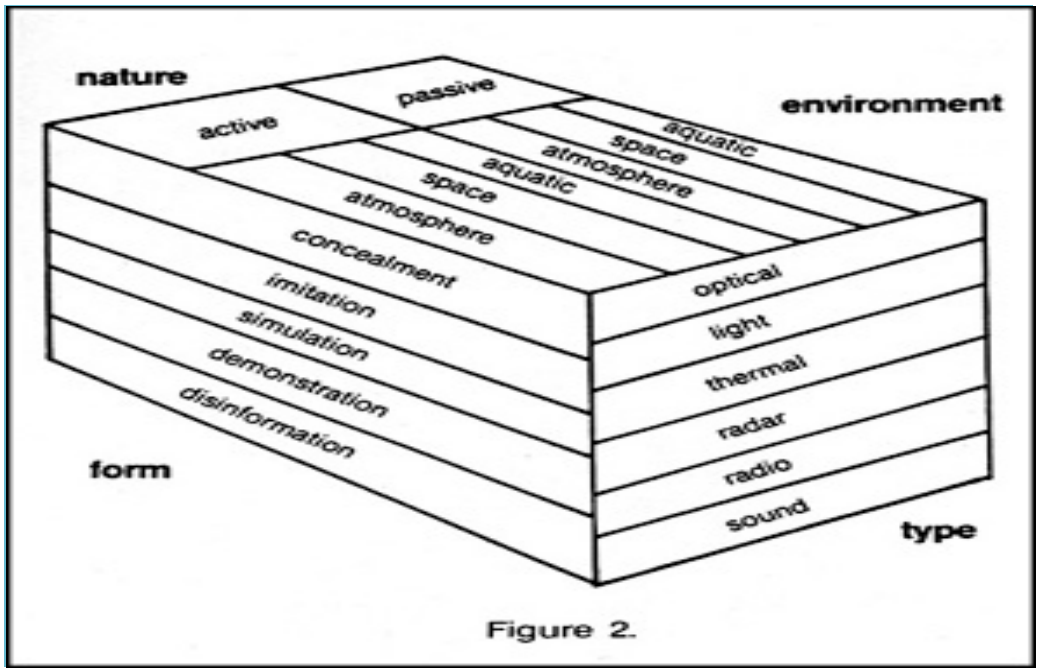
Maskirovka

The term ‘maskirovka’ has a special place in Russia’s military thought . It has been most commonly translated into English as ‘the camouflage’. Charles Smith writes that one of the obstacles that Westerners have come across while analyzing the Soviet/Russian military thought is an exact translation of the word. The English speaking West has translated the word into terms like’camouflage’, ‘concealment’, ‘deception’, ‘imitation’, ‘disinformation’, ‘security’, ‘feints’, and ‘simulation’. But the meaning is actually the sum of all these terms because maskirovka is a complex term, which has a broad meaning (Smith 1988). The Central Intelligence Agency of United States defines maskirovka as a strategy whose aim is to prevent an adversary

from discovering one's intentions by deceiving him about the nature, scope, and timing of an operation. [40] According to Smith, whether maskirovka carries within it various forms and is not of singular nature.

The following diagram gives the characteristics of maskirovka given by Charles Smith

Figure No. 4.2: Characteristics of Maskirovka



Source: *URL: http://www.airpower.au.af.mil/airchronicles/apj/apj88/spr88/smith.html.*

The diagram depicts that maskirovka can be classified on the nature, form, environment, and type.[41] On the basis of nature, it can be classified into active and passive. Similarly, on the basis of forma, it is of five types:

- Concealment: When maskirovka is of concealment form, then its purpose is to eliminate or reduce the detection of troops, weapons, and positions.
- Imitation: This form of maskirovka tactic involves producing an imitation of one's asset/s to make the enemy believe that it is the real one.

[40] Central Intelligence Agency is an external intelligence organization of United States of America. For the term maskirovka , see the C.I.A. website, URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no1/article06.html.

[41] For the classification, see Smith(1988)

URL: http://www.airpower.au.af.mil/airchronicles/apj/apj88/spr88/smith.htm

- Simulation: This is similar to imitation. It involves simulating a exercise so that the enemy is trapped into believing that something of their interest is going on within their sight.
- Demonstration: This involves doing something to divert the enemy attention.
- Disinformation: This involves sending false information or reports.

  Then, on the basis of what is used for accomplishing task, maskirovka can be:
- Optical: Using lights
- Thermal: Using heating process
- Radar: This is used to avoid detection by the radars of the enemy
- Sound: This can be used mainly for simulation, and demonstration
- Radio: This can be especially useful for demonstration and disinformation

  Finally, maskirovka can be used in all three kinds of environment that is aquatic, space, and atmosphere (Smith 1988).

Kenneth Keating gives a detailed definition of maskirovka from the perspective of camouflage. According to him, the term, which is translated as 'camouflage', means a system of measures designed to deceive and confuse the enemy, to reduce the effectiveness of his reconnaissance systems, and is a response to the challenge of technology. He further writes that Soviets have the knack for employing camouflage at strategic, operational, and tactical levels. The strategic camouflage is achieved by the Supreme High Command, and is aimed at disorienting the enemy regarding the true purpose of its army. Operational camouflage is achieved by the commander who is in the front by ensuring secrecy regarding some impending operation, its length, extent, dimensions, and duration. Finally, tactical camouflage is achieved at even lower level through the concealment of disposition of forces. In addition to this, the principles followed by the Soviets in use of camouflage are:

- Activity: It means doing something to deceive the enemy
- Conviction: This means making the fake appear very real
- Continuity: This refers to timely and constant execution of camouflage activity
- Variety: This means applying various kinds of camouflage, in order to avoid revealing any kind of pattern of camouflage to the enemy (Keating 1982).[42]

[42] See 'Maskirovka: "The Soviet System of Camouflage" by Kenneth Keating. This is the title of a research project undertaken by Kenneth Keating for the fulfillment of student requirement for

The common factor in these descriptions of the term maskirovka, is the factor of 'deception'. Deception is, therefore, either the goal of maskirovka or the instrument of it, and sometimes it is both the goal and the instrument.

One of the most famous instances of use of maskirovka by the Soviets was the Operation Bagration by the Soviet Army in June 1944 against the army of Nazi Germany[43] during Second World War. The aim of the Red Army was to recapture the Byelorussia[44] from the Nazi Army. They used the strategy of maskirovka , by making the Nazi Army believe that the Soviet offensive could come only from direction , other than that of Byelorussia. The Soviet Command ensured that the Army Group Centre of Nazi Army, which was present in Byelorussia, picked up the wrong signals. They did this by feigning preparation for a summer offensive from the northern Ukraine side, when they were actually preparing for the reconquest from the other direction for the recapture of a region which they called as 'Byelorussian Balcony'. As the Soviets had expected, the Germans took the bait and did everything that could weaken the Army Group Centre stationed in the Byelorussia. They poured most of their armour reserves into the Northern Ukraine. The powerful and most effective formation called LVI Panzer Corps was transferred to Northern Ukraine due to which the Army Group Centre at Byelorussia lost considerable armour reserves, and what followed this is now significant part of history. The Soviets as per their real plan attacked from the Byelorussian side and smashed 28 German divisions, and Germany lost 350000 soldiers, and pushed out German forces from the Byelorussia.[45]

Relation between Reflexive Control, Maskirovka, and Cyber Warfare

The common thread that runs through Reflexive Control and Maskirovka is the factor of knowledge. It is the knowledge that enables a party to draw up a model of Reflex

---

successful completion of overseas phase of training of the Department of Army's Foreign Area Officer Program, of United States.
URL: www.dtic.mil/dtic/tr/fulltext/u2/a112903.pdf

[43] Germany during the rule of Nazi party came to be called as Nazi Germany, and so Nazi Army here means the German Army.

[44] Byelorussia, here means, the area that constituted one of the fifteen constituent republics of Soviet Union. It was one of the Soviet Republics that was occupied by German forces during the Second World War. After the disintegration of Soviet Union, Byelorussia was renamed as Republic of Belarus.

[45] See "The Red Army Deception: the destruction of German Army Group Centre",
URL: http://www.globalsecurity.org/military/library/report/call/call_3-88_histp.htm

Control, and it is the degree of knowledge that enables a party to deceive or be deceived. However, it is not clear that to what extent this same factor is crucial in cyber warfare. Russia has solved this confusion by adopting an approach that does not require this question at all. Theirs is an approach that does not see cyber warfare in total isolation. For Russians, it is the Information Warfare that constitutes the bigger circle, and cyber warfare has to be seen as a part of that bigger circle. Regarding Russian understanding about this emergence of cyber warfare, Keir Giles writes:

> Debates in the West over the nature of cyber conflict are followed with interest in Russia, but are not mirrored in the Russian public narrative. Considerations of whether cyberspace is the "fifth domain" for warfare, or simply is a common factor to the other four, do not feature in discussion visible in open spaces, except in citations of Western thinking- in fact the word "cyber" is strikingly absent from home grown Russian analysis, which tends to use the term to describe U.S. or Chinese activities. Instead the Russian view of "information war"(Informatsionnoye protivoborstovo, informatsionnaya bor'ba, or increasingly commonly informatsionnaya voyna) is a more holistic concept than its literal translation suggests, carrying cyber operations within it alongside disciplines like electronic warfare(EW), psychological operations, strategic communications and Influence. In other words, Russia views cyber capabilities as tools of information warfare, which combines intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities. (Giles2011:46).

In support of development of such approach towards cyber warfare strategies, Russia has taken several steps at various levels, at policy level as well as at the doctrinal level[46]. At the doctrinal level, it has the understanding given in the points below:

(1) Firstly, the Military doctrine of Russian Federation takes cognisance of the information related threat. Russia's Military doctrine as approved by Russian Federation Presidential Edict, dated 5 February, 2010, counts information related threats as one of the main internal military dangers. Firstly, it defines this internal military danger as- "The disruption of the functioning of organs of state power, important state and military facilities, and the informational infrastructure of the Russian Federation."[47]

[46] Doctrinal level understanding reflects in general a state actor overall understands of an issue, problems, threats, and changes. The understanding is usually meant for achieving long term goals, and not for fixing short term problems. Therefore, a doctrinal understanding is one of the keys to understand a state actor's approach towards a changing military and security scenario. The doctrinal understanding is also significant for the fact that since it is meant for long term goals of state, and by virtue of that, any change that takes place in it, is a major shift.

[47] See the heading "The Military Dangers and Military Threats to the Russian Federation" in "The Military Doctrine of the Russian Federation" , as approved by the Russian Federation Presidential edict on 5th February, 2010, p.4

(2) Secondly, the document also defines the information related threats as one of "the main military threats", and defines it as: "The impeding of the operation of systems of state and military command and control of the Russian Federation , the disruption of the functioning of its strategic nuclear forces , missile early warning systems , systems for monitoring outer space , nuclear munitions storage facilities , nuclear energy facilities , atomic and chemical industry facilities , and other potentially dangerous facilities."[48]

(3) In addition to this, the doctrinal document also displays an understanding of the new features of modern conflicts that involve the information dimension. It says: "Modern military conflicts have the feature of prior implementation of measures information warfare in order to achieve political objectives without the utilization of military force and subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force."[49]It adds to this point by saying: "Military actions will be typified by the increasing significance of precision, electromagnetic, laser, and infrasound weaponry, computer controlled systems, drones and autonomous maritime craft, and guided robotized models of arms and military equipment."[50]

The 2010 Doctrine is the latest doctrinal understanding, after the cyber conflict with Georgia, during the 2008 South Ossetia and Abkhazia armed confrontation in 2008. But the word 'cyber' is missing from the document. Rather, there is a direct reference to the information related threats, conflicts, and weapons. In point (1), it has spelled out the meaning of the information threat. This is followed by its own perception regarding what it considers to be its main vulnerable information assets like military command and control systems, the systems that operate nuclear weapons, outer space, and atomic industries. In the next point, that is point (3), it spells out its understanding of the changed scenario which has come about in the wake of emergence of Information related dimensions in conflict. However, the word 'cyber' is once again curiously missing. At the first glance, such an omission appears to be a reflection of an absence of a solid approach towards the cyber warfare strategies, but drawing such

[48] Ibid , p.5.
[49]See "The Military Doctrine of the Russian Federation" , as approved by the Russian Federation Presidential edict on 5th February, 2010, p.6
[50] Ibid

an inference from the doctrinal document rests on a weak foundation, because an approach can be:

(a) A narrow approach or a 'New Entity' approach: This approach lays emphasis on how the new technology (here, the new technology is related to field of computing and cyber space) changes the way war is fought. In this approach, the tendency is to see the phenomenon as new thing, and usually new terminologies are provided for it, for instance, cyber warfare, cyber conflict, and cyber weapons.

(b) A broad or holistic approach: In this approach, the new phenomenon is integrated with some already existing understanding understanding, in order to look at the picture in a more holistic way, and by virtue of this, this approach has undertones of conservative approach.

As per the classification of the approaches, Russia falls in the second category because firstly, it has so far resisted the temptation to include the term 'cyber warfare' officially at doctrinal level. Secondly, it has just innovated its old understanding of Reflexive Control and Maskirovka by giving the term 'information'. This term enables Russia to bridge the gap between old (that is the understanding on Reflex Control and maskirovka), and new (that is, cyber warfare). For instance, Russian military thinker, Leonenko believes that Reflexive Control theory and cyber technologies are integrated. According to him, the use of computers could both strengthen and weaken the use of Reflexive Control Theory. It can weaken the effectiveness of Reflexive Control by making it easier to process data and calculate options, allowing an opponent to see through the actions of the other actor. On the other hand, the arrival of computing technology can strengthen the effectiveness of Reflexive Control, because over-reliance on computing is likely to take away the human intuition from the decision making capabilities of the opponent (Thomas 2009: 478).

At the policy level also, Russia has emphasised on an integrated and holistic approach towards cyber warfare strategies. This is manifested in its Information Security Doctrine that was developed in 2000.

Information Security Doctrine, 2000

In taking out its Information Security Doctrine in 2000, Russia took the first concreted step at the policy level to develop an approach towards cyber warfare. The timing of its release was significant for the reason that Russia was experiencing a beginning of its resurgence under the charismatic leadership of Putin, and the cyber warfare as a concept had finally emerged . This doctrine is so comprehensive, and so holistic that it is impossible to envisage a Russian understanding on cyber warfare minus its understanding on information. It defines Information Sphere as an : "Assemblage of information, information infrastructure, entities engaged in collection, formation dissemination and use of information and a system governing public relations arising out of these conditions. The information sphere as a system forming factor of societal life actively influences the state of the Russian political, economic, defense and other components of Russian Federation security."[51]

The definition of 'information sphere' itself is so broad that it includes information as an idea, but also the physical infrastructure of information, under which the cyber systems can be categorised. In addition to this, the doctrine lists certain kind of threats to the information security of Russia. They are as follows:

(a) Threats to constitutional rights and freedoms of man and the citizen in the area of spiritual life and information activities, to individual, group and public consciousness and to Russia's spiritual revival.
(b) Threats to information support to Russian Federation state policy.
(c) Threats to Russian information industry (including informatization, telecommunication, and communication facilities) development, to the satisfaction of domestic market requirements with its product and its entry into the world market, and to the accumulation, storage reliability, and effective utilization of national information resources.
(d) Threats to the security of information and telecommunications systems and facilities whether already deployed or being set up in the territory of Russia. [52]

[51] See 'Information Security Doctrine of the Russian Federation', *as approved by President of Russian Federation Vladimir Putin on September 9, 2000* , URL: http://www.idsa.in/eurasia/resources.

[52] See Information Security Doctrine of the Russian Federation', *as approved by President of Russian Federation Vladimir Putin on September 9, 2000* , URL: http://www.idsa.in/eurasia/resources.

The threats are listed in such a way that cyber threat arising out of some communication facilities are not seen in isolation from threat to individual, society , and state in the information sphere. The doctrine has also provided in detail the classification of threats. In the whole classification here, it is the point (d) that is directly related to the cyber space, and can even be called as Russian insight into cyber threats , warfare and warfare strategies. The doctrine, further classifies the point (d), by including the following under it[53]:

- Illegal information gathering and use.
- Information processing technology violations.
- Insertion into hardware and software products of components realizing functions not envisaged by documentation for these products.
- Development and distribution of programs that upset the normal functioning of information and information technology systems, including information security systems.
- Destruction, damage, disturbance of, or electronic attack against information processing, telecommunication, and communication systems and means.
- Attacks on password key protection systems for automated information processing and transmission systems.
- Discreditation of cryptographic information protection keys and means.
- Technical channel information leaks.
- Implantation of electronic intercept devices into information processing , storage and transmission hardware via communication channels or into office premises of government bodies, enterprises, institutions or organizations under whatever form of ownership.
- Destruction, damage, disturbance, or theft of machine processable data carriers.
- Interception of information in data transmission networks or on communication lines, deciphering of this information and foisting of false information.
- Use of uncertified domestic and foreign information technologies, information protection means and informatization, telecommunication and communication facilities in setting up and developing Russian information infrastructure.
- Unsanctioned access to information contained in databanks and databases.

[53] Ibid, See the elaboration of point titled ‘Threats to security of information and telecommunications systems and facilities’.

- Breach of lawful restriction on information dissemination.

The points given indicate the Russian understanding of cyber threats to the society, individual and state. Each point talks about a vulnerability that the cyberspace increases, when a country is dependent on it in various spheres. Russia, on the basis on its own assessment has come out with its list of vulnerable points in the form of these points, that might become target of a cyber attack by state or non-state actor. The points also indicate that the Russia has made such a broad Information doctrine that the cyberspace related issues have been subsumed under it.

This crucial place of the information as a concept is almost like a pivot around which the Russian cyber warfare discourse revolves. Given the fact that Russia has two intellectual legacies in the form of concepts of Reflexive Control Theory and Maskirovka, it is natural for Russia to intertwine the two concepts with the cyber warfare principles. T.L. Thomas opines that for Russians, the cognitive aspect is so important that they prefer to keep the cyber warfare related matters also within the information circle of information warfare. In his another work (Thomas 2009), Thomas also writes about how the theory of Reflexive Control could not benefit the Soviets much, despite of the excellent understanding that they possessed regarding this concept. The very fact that Soviet Union was tempted to enter into an arms race with U.S. by the latter, and was later exhausted economically, shows that Soviets failed to see through the game of reflexive control initiated by the U.S. (Thomas 2004).

However, despite its failure of Reflexive Control method, as stated by Thomas, Russia has retained the cognition factor in its approach towards cyber warfare strategies by keeping the centre of discourse as ‘information’. What kind of choices, then, has Russia made to use cyber warfare strategies in conflict situations, given its understanding? There are three major conflicts in the Post-Soviet period, in which Russia made use of cyber warfare strategies for different purposes, and used various strategies.

Russia’s Cyber Warfare Strategies against Chechens

The first thing that Russia confronted after the disintegration of Soviet Union was a flood of information that were either highly pro-West, or was encouraged by the

West. In the second half of the 1990s decade, when an economic crisis was on in Russia, the country had to turn its attention to the crisis. So a major part of its attention was absorbed by the crisis. Adding to its problems was the conflict with Chechens.[54] In the initial phase of the conflict, the Chechens had the upper hand in showing its side of the story. The Chechens used the press and cyberspace to their advantage by disseminating information regarding how the Russian Federal government was committing atrocities against the Chechens. Graem Herd writes-

> For the Russian Federation, the first Chechen war (1994-96) represented military disaster and national humiliation. This failure has been ascribed to a number of factors. It was generally recognized that the media 'war' was not contested – federal media was non-existent, Russian and international (Western) public support weak or non-existent, and considerations of the relationship between presentation and policy formulation completely uncoordinated. Russia failed to gain and hold an information advantage or 'superiority' over the Chechens fighters…Key television channels , such as NTV , highlighted blatant discrepancies between the government line on Chechnya and live video footage of dead , maimed and captured Russian soldiers and candid interviews from the front; this undermined government credibility . As Igor Malashenko, the director of NTV, sardonically noted of government news reports: 'They do not care how many people are killed .But they do care how many dead bodies are shown on television 'Thus public opinion, that clearly did not support the first campaign, hindered the government's ability to fight effectively and justify the war in both domestic and international arenas, so undermining the perception of Russia as a state in transition towards democratic consolidation. (Herd 2002: 110-111).

However, in the second phase of the conflict with Chechens that began in 1997, the Russian government seized the opportunity to fight the Chechens in the information sphere as well, by employing cyber warfare strategies. The sole aim of these strategies was to use cyberspace to counteract the propaganda of the Chechen groups in cyberspace that sought to malign the Russian policy. Moscow adopted the strategy of both controlling the amount and type of information being released. There were Chechen run websites like kavkaz.org, along with that was based in Malaysia. Russians counteracted this first by disseminating information through websites like 'infocentre.ru' that prescribed how reporters should report the conflict.State

[54] Chechenya is a region in the South west part of Russia that borders Georgia. It is inhabited by the ethnic group called Chechens. During the Soviet period this region was brought under the control and jurisdiction of the Soviet Union. However, as soon as the Soviet Union broke up, the region was caught by the wave of separatism. This fuelled a conflict between the Federal government of Russian Federation and the ethnic guerrilla groups in the region. Often known for its protracted nature, this conflict was fought in two phases. The first phase coincided with the presidency of Yeltsin. It began from 1994, and lasted till 1996. The first phase ended with a cease fire agreement, and Aslan Maskhadov, the separatist leader, becoming the President of the Chechen Republic. However, tensions soon started in 1999. This second round of tension led to renewal of conflict between the Russia's federal government and the separatists. Tthis second phase also lasted for nearly two years and coincided with the presidency of Vladimir Putin.

controlled radio and television broadcasts were also used to press the Russian side of the story about the conflict. On the other side, the Chechens kept giving their version of the events from the conflict zone. Then, in the year 2002, Chechen leaders claimed that two of their main sites kavkaz.org and chechenpress.com had crashed under the attacks by the hackers. The site'kavkaz.org' was based in United States, and after making public the news about the hacking , the spokesperson for the Chechen website said that he was amazed that Russian security forces could act so freely on U.S. territory. The Chechens claimed that the website had been hijacked by the FSB hackers. In response to this attack, Chechens moved the information to another site called 'kavkazcenter.com', but that site also came under the attack by hackers (Chang 2004).

Therefore, the cyber warfare strategies employed by Russia in the latter half of its conflict with Chechens aimed at cutting the flow of the information that the opponent was feeding to lower the morale of the people, the armed forces and also to malign the Federal government. President Putin towards the end of the conflict awarded some journalists also, and made a cryptic comment, that referred to Russia's information warfare only slantly. He said, "What created that bloody mess which you and I observed during the so called first Chechen campaign was a lack of understanding of what was happening. We ourselves could not come to grips with what those events meant."This was a statement that belied confidence, which had come after Russia had successfully dealt with the problem by employing the cyber warfare strategies by integrating it with their overall information campaign against Chechens.

Estonia 2007: Executing PSYOPS with Cyber Warfare

Psychological Operations (PSYOPS) are the most preferred resorts for the state actors where the aim is to just cow down the opponent, either through display of one's power, or through the exposure of opponent's weakness to the rest of the world. In 2007, Russia was placed in a situation where it could neither remain silent nor could it choose the option of militarily cowing down the opponent (that is, Estonia).[55]The conflict that had arisen was of a nature which demanded a reaction that had both the audacity and the subtleness. By flaming passions through a proposal to remove a Soviet era statue, Estonia had fired a psychological offensive against Russia. The

[55] See Chapter 3 for more details on Russia-Estonia Conflict in 2007.

response of Russia could not have remained completely mild (for instance, a verbal condemnation), or an extreme response of a military action. So, the middle path that emerged before Russia was the 'psychological cowing down'. This of course required an integrated approach. Therefore, when the Distributed Denial of Services attacks took place, Estonia was crippled temporarily. At the same time, the opponent could only succeed in establishing that the attacks had the Internet Protocol addresses in Russia as the origins. They could not arrive at a firm conclusion that Russian Federal Security Services had done so. These attacks were also accompanied by suspension of rail deliveries of raw materials and passenger services between the capitals of two countries. [56] The results of the combined attacks were as follows:

(1) The sites offering various services became inaccessible, rendering ordinary people in Estonia helpless.
(2) Estonia had to cut itself from rest of the world temporarily, resulting in economic losses.
(3) It created messy situation where people were not sure how to respond to wrath of various hackers from Russia, who had poured out their anger against the Estonian government's decision to remove the Bronze Statue.
(4) Russia came out unscathed, for its role in attacks could not be conclusively established even when it appeared so evident to the world.
(5) Russia succeeded in hitting Estonia where it hurt the most that is the extensive cyber networks that controlled the economy and administration. The government and Parliament websites were targeted and defaced, thereby causing a virtual paralysis for some time.[57]

Russia-Georgia Cyber Conflict: Cyber Warfare Strategies with Kinetic Attacks[58]

The Russian cyber offensive against Georgia can be termed as the only unique example of cyber warfare so far because:

[56] For the events that happened during cyber attacks in Estonia, see "Estonia and Russia: A Cyber-riot", The Economist, (May 10,2007), URL: http://www.economist.com/node/9163598?story_id=9163598

[57] Estonia is one of those countries that have a very dense and extensive cyber networks. Its banking sector is especially completely dependent upon the functioning of cyber networks.
[58] Kinetic Attacks are meant for physical destruction .

a) It was one such conflict that involved a clear use of cyber space against the adversary, in a situation of military conflict between two states.
b) It involved the use of cyber warfare strategies in consonance with the use of kinetic attacks to push the enemy further.

This is a case in which cyber warfare strategies were used both in the prelude to actual military conflict as well during the conflict. In the prelude, that is two weeks before the actual military clash began, the Georgian sites began to get DDOS attacks. It happened in June 2008. The attacks were carried out using botnets, which are a network of infected computers. Then on 20 July 2008, the website of President of Georgia was also served with DDOS attacks, and the site was forced to shut down for 24 hours. On the day when the actual conflict began, the websites of key ministries were served with DDOS. The targeted ministries were foreign, finance, and defence. Along with these, the websites of Georgian Parliament were also attacked. Two hacker forums Stopgeorgia.ru, and Xakep.ru played very active role in carrying out these DDOS attacks. Therefore, even as tanks were Russian tanks were rolling, and naval blockade was being done to push the Georgian forces out of South Ossetia and Abkhazia, the cyber attacks remained on to put the psychological pressure on the Georgian government(Heickero 2010: 43-45)

Maskirovka and Development of Logic Bombs

In the current context of cyberspace, the three components of maskirovka, that is concealment, camouflage, and deception can be really helpful in imparting destructive power to codes in computer that can bring destruction in the physical space. This is possible with the use of logic bombs .Logic Bombs are the programs that have been inserted with a set code that will bring about one or all of the following changes:

- Cause the machine or system which is running with the help of that software to suddenly stop after a period of time.
- Cause the system to slow down.
- Cause the destruction of files that are stored.
- Cause the fluctuations in speed /rate/pace/frequency of a system to fluctuate, thereby causing an accident, blast, explosion or any industrial sabotage. (Heickero 2010:21-22)

These are the malwares that function on the basis of concealment, camouflage, and deception. It is concealed because for some time the program might function without any harm. It uses camouflage because it comes with the software that is supposed to function for running some systems, and it uses deception because it deceives the user until it starts showing the harmful effects.[59] Russia is moving in the direction of developing these weapons for an offensive cyber attack strategy.[60]

Conclusion

Russia has understood the concept of cyber warfare with the help of its existing knowledge, that is Reflexive Control Theory and the concept of Maskirovka. As a result, Russia's approach towards cyber warfare is information oriented, and is very broad. It takes into account the cognitive aspect of the human psychology to devise warfare strategies. As a result, the most important components like PSYOPS of Russia's cyber warfare strategies revolve around using information in the cyberspace to cut the information flow of the adversary, to cow down the opponent, to put pressure on the opponent to withdraw or cause it loose the morale. All three instances- the offensive against Chechens, Estonia, and Georgia indicate Russia's propensity to integrate the use cyberspace against adversary to gain an information advantage or cut the information advantage of the adversary. It is not limited to technical aspects of cyberspace and is wholly integrated with the cognitive aspect of human behaviour. Therefore, Russian strategies of cyber warfare require one to look beyond the machines, into the human psyche. In one sense, Russia's approach is an intellectual approach towards cyber warfare.

[59] Ibid, p.21-22

[60] See "The Brave New World of the 5 Day War", a discussion on Russia's view on Information Warfare.
URL: nationalstrategies.com/pdf/publicsafety_govsec_5daywar_joyal.pdf

Chapter 5

One of the factors that give a maximum sense of security to a state actor is the thought of having control over its domain, and it has been popularly understood and termed as *sovereignty.* This idea of sovereignty rests on definite boundaries, both in minds and in physical space. However, over a period of time, a mammoth idea of Cyberspace has posed a challenge to the position held by the idea of the Sovereignty. Attempts have been made to define it, study its components and its characteristics, but what these attempts have given to humanity is a *collage of pictures.* This means that numerous meanings have come out, yet the concept itself remains undefined. Its characteristics have puzzled the scholars, because it defies the way a physical object can be defined. What have come out are the following things:

- Cyberspace is neither completely virtual, nor is it completely a physical object.
- Cyberspace is an idea, a state of mind, and a psychological connection with the other person on net.
- Cyberspace is a network of computers.
- Cyberspace is only virtual space, which means that it does not belong to realm of physical objects.

In other words, the word cyberspace has plural meanings, and it has been associated with both the realm of virtual things such as, idea, state of mind, psychological connection, and physical objects (for instance, computer networks). This quality of being both virtual and physical imparts cyberspace the power to criss-cross the boundaries of state. It enables cyberspace to share the space which has hitherto been the preserve of state actors. For instance, the growth of cyberspace has given birth to the practice of hacking of sites that belong to governments and that too with great ease. An amateur hacker, who possesses basic skills of computing and hacking, can easily cause a temporary paralysis in the administration of an office, without even getting caught. This implies that cyberspace has created an insecure space for the state actors, where they might end up only repairing the damage without succeeding in catching the actual culprit. This is a space where their mighty structure faces a challenge by the very virtue of being present in such a space.

Then, there is a need to understand why the concept of cyber warfare having involvement of state actors, has emerged, when the very concept of cyberspace is a challenge to state. This is like a puzzle, because the idea of cyberspace challenging state and the beginning of cyber warfare are anti-thetical to each other. This means that the same phenomenon is appearing to both strengthen and weaken the state. Now, there are two ways to explain it:

(1) The kind of cyber warfare that has emerged has no involvement of any state actor, organisation, or structure.
(2) Cyberspace weakens some aspects of state actors, and strengthens some other aspects.
(3) The cyber warfare having active involvement of state actors is a symptom of states' response to the workings of cyberspace.

On the basis of empirical evidence, the first explanation cannot be defended because quite a large number of state actors have actively gone for the option of waging cyber warfare against the opponent. The first chapter had given the instances cyber warfare being actively pursued by state actors, or cyber warfare strategies being developed by them. Therefore, this point cannot withstand the empirics that show the active involvement of state actors. The second line of explanation attempts to give a very comprehensive explanation, but lacks the clarity. Its second drawback is its faultline that is inclusion of two opposite phenomenon with a common factor to explain both. It is a kind of explanation that says *increase in 'x' leads to increase in 'y',* and at the same time *increase in 'x' leads to decrease in 'y'.*

It is the third point which this study has taken up for examination. For this purpose, a hypothesis has been devised for scrutinising the point to explain why there is a phenomenon of cyber warfare when the cyberspace has been assumed to be a challenge to state. So, here comes the first hypothesis- *The increasing militarisation of cyberspace is a direct consequence of efforts of state actors to control the cyberspace*. There are ways to control the cyberspace- legally, militarily, ideologically, politically, and culturally. *Legally* means devising laws to include and exclude as per one's needs, choice and interests, to define crimes in cyberspace, and to develop penalty for crimes, and to sign international agreements to arrive at a common understanding on functions in the cyberspace. *Controlling ideologically*

means influencing the activities in cyberspace by disseminating ideologically oriented ideas. Controlling culturally also has a similar connotation, but it is different from an ideological control in the sense that the former seeks to develop a culture in cyberspace that helps in maintaining the domination of the powerful actor.

The fourth kind of control is a *political control*. The word political in the present context is very broad. In this context, if a state succeeds in having legal, military, ideological, and cultural control in cyberspace, then it gets the rein for political control as well. The fifth kind of control is the *military control*. In other words, these are the five ways at the disposal of the state actors to have a control over cyberspace, and each way will give its by-product.

Table No. 5.1: Types of Control over Cyberspace

Type of Control	**The By-product/s**
Legal Control	**A set of laws, legal framework that clearly defines all the aspects of cyberspace, along with complete control over the activities in cyberspace.**
Ideological Control	**Having full ideological supremacy in cyberspace.**
Cultural control	**Having domination of one's culture in cyberspace.**
Political Control	**Having legal, ideological, cultural, and military control.**
Military control	**Development of one's cyber warfare doctrines, cyber weapons, development of cyber conflicts, and cyber warfare.**

The first three chapters have brought out the following:

(1) The cyberspace appears to be a domain where various kinds of actors are active, that is non-state, and state actor.

(2) The cyberspace remains undefined legally, and so are cyber crimes.

(3) Countries have found cyberspace as a new attractive battle zone, and cyber warfare has been incorporated in the military doctrines of quite a number of countries.
(4) Cyber conflicts have already taken place.
(5) There are various kinds of cyber weapons at present. For, instance, malwares and logic bombs.

The first two findings do not show the even the signs of by-products of the first four kinds of control given in the table. On the other hand, the remaining three findings show the signs of the by-products of military control. This finding can happen in three kinds of scenario:

(1) The state actors are constantly trying to control the cyberspace in all five ways, but only the military efforts have been successful.
(2) The state actors make efforts only in military sphere, and the remaining four remain untouched.
(3) The efforts to control cyberspace through legal, political, ideological, and cultural ways are ultimately geared towards controlling it through military ways.

In all three kinds of scenario, the consequence of state efforts to control cyberspace is a militarised cyberspace. However, this is definitely subject to future developments, like emergence of widely accepted, comprehensive definition of cyberspace, along with a common understanding on rules and laws of cyber warfare, among state-actors.

The second relation that this study has sought to explain is the one between growth in information technology in defence sector, and integration of cyber warfare in Russia's warfare doctrine. In this study, it is the third and fourth chapter that have gathered some facts that pertain to both the independent and dependent variables. In order to make an impact on any sector, or sphere of economy, or any aspect of a state's life, the growth in any sector has to be consistent and constant over a period of time. Therefore, the third chapter for a large part focusses on some of the historical aspects of the developments in the field of computing during Soviet period. It contains facts that show that the Soviets did make all out efforts to weaponise the cyber technologies to an extent where the computing industry developed a separate area that catered only to defence needs. This whole industry was a legacy without which Russia, in the Post-

Soviet period could not have even envisaged possessing any kind of cyber warfare capabilities.

The counter argument to this argument could be that Russia possesses a rich legacy of Information Warfare literature in the form of Reflexive Control and Maskirovka , and these are the driving factors for Russia formulating a cyber warfare doctrine. However, this makes the picture fuzzy, instead of providing a clear explanation. Hypothetically, the factors that drive the integration of cyber warfare doctrine in Russia's warfare doctrine can be:

(1) Development of information technology in defence area.
(2) The import of scientists who work in the field of information technology.
(3) Import of defence related information technologies from another country.
(4) A pre-existing framework of Information Warfare.
(5) An experience of having bore the brunt of cyber attacks.

Firstly, those factors need to be eliminated that cannot be true in case of Russia, and here those factors are (2), and (3). If one observes defence related technological development from Soviet period onwards till the present times, it is clear that the field of computing has indigenous roots. This means that import of scientists or import of defence related information technologies cannot be consistent factors. The word consistent here means having regularity. This implies that three factors are left that vie for the same place. The fourth point is *a pre-existing framework of Information Warfare* .As has been seen in the fourth chapter, Russia does have a pre-existing framework of Information Warfare in the form of Reflexive Control Theory and Maskirovka. However, the framework that Russia possesses mainly since Soviet times is more in nature of principles and fundamentals for practising both warfare and peace time politics. They are the means to develop an approach towards warfare in general, rather than a point of ignition that will drive a technological change. It can also be added here that if information warfare framework really drives the integration of cyber warfare in a general warfare doctrine, then the cyber warfare concept would have developed much earlier.

This, then leaves the two factors, given by point (1), and (5) as two factors that can explain the problem. The factor given in point (5) appears as a potential factor for driving the integration of cyber warfare in the warfare doctrine of Russia , because

Trans-Siberian Gas Pipeline blast that happened in Soviet Union acted as a wakeup call to the Soviets. However, after eight years, the Soviet Union broke up; leaving its successor Russian Federation in a mess that haunted it for at least another seven years. These seven years were not fertile time for Russia, fertile enough for a rapid development of a cyber warfare doctrine. Therefore, the potential factor that acts as the driving factor is the development of information technology in the area of defence. This drive has been possible due to the rapid strides made by the computing industry, especially during Soviet times.

The third relation that this study hypothesizes is the relation between the central role of information in achieving victories and the conceptualisation of cyber warfare within a framework of Information Warfare .Therefore, the question that the study poses is-Does the pivotal role of information in Russia's success in its military conflicts play a role in cyber warfare being conceptualised as information warfare? For this problem, the study has relied on analysing the relevance of two things- *Reflexive Control Theory, and Maskirovka*. *Reflexive Control Theory*, as has been found in this study, is actually a key to understand one's as well as the opponent's action. Without a framework provided by a Reflexive Control model, it is not easy to envisage the merits and demerits of any kind of step in a given situation. It is one of the bases in Russian strategic thought that open the gates to Russia's thought on warfare. One of the fundamentals of this theory is to devise a model to evaluate information. This information could be anything – a gesture, sound, action , written report, initiative, and show of strength or display of vulnerabilities. Therefore, in Russia's strategic thought, evaluation of information and devising a response to the opponent is even more important than fighting the actual battle.

Maskirovka is another concept that holds a special place in Russia's strategic thought. Unlike *Reflexive Control Theory*, this is more about using the information to deceive, camouflage, divert, and conceal. It has been popularly understood as a tactic rather than as a broad strategy. However, it can be used in combination with Reflexive Control to achieve lethal results. In its *Information Doctrine of 2000*, which represents Russia's official stance on Information Warfare, these are the two things that are missing .However, it should not be misconstrued as moving away from very framework of Information , because these are things that are not meant for the benefit

of the outsiders . Strategic thoughts are obviously kept to oneself. The *Information Doctrine (2000)* only provides Russia's traditional information centric understanding about everything that happens in their surroundings. Even the concept of cyber warfare is subsumed under it.

This subsuming process does not reflect a narrow understanding of cyber warfare as a evolution of information technology. Instead, Russia sees cyber warfare as a new way to use information in the conflicts. This approach has paid off Russia in very crucial moments. The first instance is that of Chechenya conflict. The first phase of the conflict that began in 1997 was messy for Russia. Every kind of negative coverage of Russia took place -photos of Russian forces committing human rights violations in Chechnya, were amply displayed in some websites run by the rebels who were fighting Russian forces. Realising this, Russia Federal government took swift measures by combining offensive actions in cyber space along with other media to thrust its side of the story. The actions paid off the government that was thirsty for some sort of victory to boost the morale of both the forces and the people. Since, then Russia has employed cyber warfare strategies in two more conflicts - one with Estonia in 2007 and the other with Georgia in 2008. In both the conflicts, Russia tackled the conflict situation with the help of less effort.

However, it is worth pondering whether these are the victories that Russia would consider while conceptualising cyber warfare in an information warfare framework. Here, the assumption that has been made in this study will come handy. One of the assumptions in this study is that the actor is rational and learns from its past mistakes. In other words, the results from the past period are crucial in understanding the present. Therefore, it is not just these three successful cases that are crucial in Russian understanding on cyber warfare, rather all the main successes dating mainly from Second World War are the determinants of the present understanding. Russia has so far experienced that defeating the opponent in the sphere of cognition is more important than defeating him in any other sphere. This makes their concept of cyber warfare highly information centric. In one sense, Russians appear to be true believers in Sun Tzu's words-"Know your enemy, and know yourself".

References

(* indicates primary sources)

Arquilla, John and Ronfeldt, David (1997), "Cyberwar Is Coming!", in John Arquilla and David Ronfeldt (eds.), *Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND Corporation.

Apokin, I. A. (2001), "The Development of Electronic Computers in the USSR", Georg Trogemann, Alexander Y. Nitussov and Wolfgang Ernst (eds.), *Computing in Russia: The History of Computer Devices and Information Technology revealed*, Germany: Vieweg: Braunschweig.

Azarov, Serge S. and Dodonov, Alexander G. (2006), "Instrumental Corrections for a Definition of Cyberwar", Carvalho, Fernando Duarte and da Silva, Eduardo Mateus (eds.), *Cyberwar- Netwar - Security in the Information Age*, IOS Press.

Antal, John (2011), "Keeping Secrets in the Digital Era", Annual *Cyberspace Focus, Military Technology*. *Miltech*. 3/2011: 76-90.

Abrieu, Elinor (2001), "Cyberattack Reveals Cracks in U.S. Defense", *PC Plus*, May 10, 2001, URL: http://www.pcworld.com/article/49563/cyberattack_reveals_cracks_in_us_defense.html.

Banks, Michael A. (2008), *On the Way to the Web: The Secret History of the Internet and its Founders*, Apress Publications.

Buzan, Barry & Herring, Eric (1998), *The Arms Dynamic in World Politics*, Colorado: Lynne Rienner Publishers Inc.

Brzezinski, Matthew (2007), *Red Moon Rising: Sputnik and the Hidden Rivalries That Ignited the Space Age*, New York: Times Books, Henry Holt and Company.

Biegel, Stuart (2001), *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Massachusetts and London: MIT Press.

Carvalho, F. D. and Da Silva, E. Mateus (Ed.) (2006), Cyberwar-netwar: Security in the Information Age, New IOS Press Inc.

Chapman, Cameron (2009), "The History of the Internet in a Nutshell", November 15, [Online Web] Accessed 10 November 2011 , URL: http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/.

Cyberspace and Information Operations Study Center, Air University , Maxwell Air Force Base, Montgomery, Alabama, U.S.A., website. URL: http://www.au.af.mil/info-ops/perception.htm#reflexive.

Cukier, Kenneth Neil (2005), "Who will control the Internet? Washington battels the world", *Foreign Affairs*, 84(6): 7-13.

Chansoria, Monika (2010), 'Informationising' Warfare: China Unleashes the Cyber and Space Domain", Maneshaw Paper, No. 20, 2010, *URL:* www.claws.in/download.php?action=1270592252MP_20.pdf.

Cohen, Eliot A. (1996), "A Revolution in Warfare", *Foreign Affairs*, 75(2): 37-54.

Coleman, Kevin (2008), "Cyber Warfare Doctrine: Addressing the most significant threat of the 21st century", *The Technolytics Institute*. URL: www.technolytics.com/Cyber_Warfare_Doctrine_Public_Version.pdf.

Drogin, Bob (1999), "Russians Seem To Be Hacking Into Pentagon", Los Angeles Times, October 7, 1999, [Online Web] Accessed 30 November 2011, URL: http://www.sfgate.com/cgibin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL.

Dodge, Martin and Kitchin, Rob (2001), *Atlas of Cyberspace,* London: Pearson Education.

"Declassified: The Secrets of Soviet Computing", Dated 25/06/2009, *PC Plus*, URL: http://pcplus.techradar.com/2009/06/25/declassified-the-secrets-of-soviet-computing/.

Davis, Joshua (2007), "Hackers Take Down the Most Wired Country in Europe", August 21, [Online Web] Accessed 30 November 2011, URL: http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

Drezner, Daniel W. (2004), "The Global Governance of the Internet: Bringing the State Back", Political Science Quarterly, 119(3): 477-498.

Denning, Dorothy E. (2007), "Assessing the Computer Network Operations Threat of Foreign Countries", Arquilla, John and Borer, Douglas A. (eds.), Information strategy and warfare: a guide to theory and practice, Routledge.

D'Souza, N (2011), "Cyber Warfare: Remedies in International Law". URL:papers.ssrn.com/sol3/.../SSRN_ID1842984_code1660714.pdf?...1.

Eriksson, Johan and Giacomello, Giampiero (2006), "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", *International Political Science Review*, 27 (3): 221-244.

Farwell, James P. and Rohozinski, Rafal (2011), "Stuxnet and the Future of Cyber War", *Survival*, 53(1): 23-40.

Frissen, Paul (2005), "The virtual state: postmodernisation, informatisation and public administration", Brian D. Loader (eds.), *The Governance of Cyberspace: Politics, technology and global restructuring*, London and New York: Routledge.

Gerovitch, Slava (2002), *From Newspeak to Cyberspeak: A History of Soviet Cybernetics*, MIT Press.

Gumpert, Gary and Drucker, Susan J. (2007), "Mobile Communication in the 21st Century or "Everybody, Everywhere at any Time", Kleinman, Sharon (eds.), Displacing place: Mobile Communication in the 21st Century, New York: Peter Lang Publishing, Inc.

Hansen, James H. (2007) "Soviet Deception in the Cuban Missile Crisis: *Learning from the Past", Centre for the Study of Intelligence, Central Intelligence Agency*, 146 (1), [Online Web] Accessed 22 November 2011, URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csistudies/studies/vol46no1/article06.html.

Herd, Graeme P. (2002), "The Russo-Chechen information warfare and 9/11: Al-Qaeda through the South Caucasus looking glass?", *European Security*, 11(4): 110-130.

Hoisington, Matthew (2009), "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review*, 32(2):439-454.

Hughes, Rex (2007), "Bits, Bytes and Bullets", *World Today***,** 63 (11): 20-22.

Hakken, David (2002), *Cyborgs@ Cyberspace?: An Ethnographer Looks to the Future*, London and New York: Routledge.

Hollis, David (2011), "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, [Online Web] Accessed 8 December 2011, URL: http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Heickero, Roland (2010), "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations", FOI, Swedish Defence Research Agency, Division of Defence Analysis.

*Ministry of Foreign Affairs(2000), Government of Russian Federation, Ministry of Foreign Affairs, *Information Security Doctrine of the Russian Federation, Approved by the President of the Russian Federation Vladimir Putin on September 9, 2000*, URL: http://www.idsa.in/eurasia/resources.

"Intro to Protocol Wars" by Roger Scantlebury (Video), dated 2011, produced by Jon Plutte and Aimee Gardner, copyright owned by Computer History Museum, [Online Web] Accessed 12 Novmber 2011, URL: http://www.computerhistory.org/revolution/networking/19/376/2326.

Interview: John Arquilla, March 4, 2003. *Frontline*, URL: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html

Keir Giles (2011), "Information Troops" – a Russian Cyber Command? , C. Czosseck, E. Tyugu, T. Wingfield (eds.), *3rd Conference On Cyber Conflict* , Tallinn , Estonia, CCD COE Publications, , [Online Web] Accessed 12 Novmber 2011, URL: http://www.ccdcoe.org/publications/2011proceedings/2011_Proceedings.pdf.

Jordan, Tim (2003), *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, London and New York: Routledge.

Jassem, Harvey (2007), "Municipal WI-FI Comes to Town", Sharon Kleinman (eds.), *Displacing Place: Mobile Communication in the Twenty First Century*, New York: Peter Lang Publishing Inc.

Joyal, Paul M. (2011), Russia- Georgia cyber war: The Brave New World of the 5 Day War Where Cyber and Military Might Combined for War, URL: http://www.slideshare.net/pjoyal/govsec-georgia-2008-cyber-war.

Joyner, Christopher C. and Lotrioonte (2001) "Information Warfare as International Coercion: Elements of a Legal Framework", *Ejil*, 12(5): 825-85.

Keating, Kenneth C. (1982), Maskirovka: The Soviet System of Camouflage, Student Research Report, U.S. Army Russian Institute, APO, New York, Publisher: Defense Technical Information Center, URL: www.dtic.mil/dtic/tr/fulltext/u2/a112903.pdf.

Kojevnikov, Alexei B. (2004), Stalin's *Great Science: The Times and Adventures of Soviet Physicists*, London: Imperial College Press.

Kuehl, Daniel T (2009), "From Cyberspace to cyberpower: Defining the Problem", in Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz (eds.), *Cyberpower and National Security*, Potomac Books Inc.

Karpova, Vera B. and Karpov, Leonid E. (2011), "History of the Creation of BESM: The First Computer of S.A. Lebedev Institute of Precise Mechanics and Computer Engineering", in John Impagliazzo and Eduard Proydakov (eds.), *Perspectives on Soviet and Russian Computing*, New York: Springer.

Lipayev, Vladimir (1997), "History of Computer Engineering for Military Real Time Control Systems in the U.S.S.R." , Russian Virtual Computer Museum, [Online Web] Accessed 12 November 2011, URL: http://www.computer-museum.ru/english/milhist.htm.

Loader, Brian D. (2005), "The governance of cyberspace: Politics, technology and global restructuring", in Brian D. Loader (eds.), *The Governance of Cyberspace: Politics, technology and global restructuring*, London and New York: Routledge.

Lonsdale, David J. (1999), "Information Power: Strategy, Geopolitics, and the Fifth Dimension", *Journal of Strategic Studies*, 22(2-3): 137-157.

Libicki, Martin (1999-2000), “Rethinking War: The Mouse's New Roar?” *Foreign Policy*, No. 117 (Winter, 1999-2000): 30-32+34-43.

Libicki, Martin C (2009), *Cyberdeterrence and cyberwar* , RAND Corporation.

Luke, Timothy W (2001), “Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism”, *Alternatives: Global, Local, Political*, 26(2):113-142.

Maliukevicius, Nerijus (2007), Geopolitics and Information Warfare:Russia’s Approach, *Lithuanian Annual Strategic Review* 2006, *URL*:http://www.isn.ethz.ch/isn/DigitalLibrary/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=120650.

Meyer, Paul (2011), “Cyber Security through Arms Control: An Approach to International Co- Operation”, *The Russi Journa*l, 156(2): 22-27.

*McAfee Virtual Criminology Report: Cybercrime versus Cyberlaw, McAfee Inc. URL: http://www.ifap.ru/pr/2008/n081212b.pdf.

Murray, Williamson (1997), “Thinking About Revolutions in Military Affairs”, *JFQ* Summer (1997), *URL*: http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA354177&Location=U2&doc=GetTRDoc.pdf.

Madhok, Vikas (2010), Ade- Novo Look at China’s Cyber Warfare Capebility from an Indian Context”, *Trishul*, 23(1):25-36.

Myrli, Sverre (2011), “NATO and Cyber Defence”, *Military Technology*, March 2011: 86-90.

Carr, Jeffrey (2010), *Inside Cyber Warfare*, Sebastopol: O’Reilly Media.

*Minutes of the Session No.1 of the Science Council of the Institute of Electronic Technology and Heat Power Engineering Ukrainian Academy of Science, held on 8 January, 1951, [Online Web] Accessed 6 November 2011, URL: http://ukrainiancomputing.org/LEBEDEV/TXT/protocol.html.

Naim, Moises (2005), “Net Effect: Web Sites That Shape the World.” *Foreign Policy*, 146 (Jan- Feb): 92-95.

*****Project Grey Goose Phase II Report: The evolving state of cyber warfare, March 20, 2009. URL: www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report.

*Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats. January 21, 2010. *URL:* http://dataclonelabs.com/security_talkworkshop/papers/25550091-Proj-Grey-Goose-report-on-Critical-Infrastructure-Attacks-Actors-and-Emerging-hreats.pdf.

Post, David G. (2009), *In Search of Jefferson's Moose: Notes on the state of Cyberspace*, New York: Oxford University Press.

Portnoy, Michael and Goodman, Seymour (eds.) (2009), *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, New York: Springer.

Putney, Diane T. (2004), *Airpower Advantage: Planning the Gulf War Air Campaign 1989-1991*, Washington: Air Force History and Museums Program, United States Air Force.

*President of Russian Federation Office (2010), Government of Russian Federation, *The Military Doctrine of the Russian Federation*, as approved by on 5 February 2010 by Presidential Edict, URL: http://www.idsa.in/eurasia/resources.

Rabinovich, Zinoviy L. (2011), "The Work of Sergey Alekseevich Lebedev in Kiev and Its Subsequent Influence on Further Scientific Progress There", in John Impagliazzo and Eduard Proydakov (eds.), *Perspectives on Soviet and Russian Computing*, New York: Springer.

Reid, Elizabeth (2005), "Hierarchy and power: social control in cyberspace", in Mark A. Smith and Peter Kollock (eds.), *Communities in Cyberspace*, Routledge: London.

Safire, William (2004), "The Farewell Dossier", *The New York Times*, February 2, 2004, [Online Web] Accessed 30 October 2011, URL: http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html.

Smith, Charles (1988), "Soviet Maskirovka, *Airpower Journal*, Spring, URL: http://www.airpower.au.af.mil/airchronicles/apj/apj88/spr88/smith.html.

Shabazz, Daim (1999), "Internet Politics and The Creation of A Virtual World", *International Journal on World Peace*, 16(3): 27-39.

Santa Monica, CA (1993), “Cyber War is Coming!”, *Comparative strategy*, 12: 141-165.

Sharma, Deepak (2011), “China Cyber Warfare Capability and India’s Concerns”, Journal of Defence Studies, 5(2): 62-76.

Sharma, Amit (2009), “Cyber Wars: A Paradigm Shift from Means to Ends”, Christian Czosseck and Kenneth Geers (Edited), *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam and Berlin: IOS Press.

Shakarian, Paulo (2011), Stuxnet: Cyberwar Revolution in Military Affairs”, *Small Wars Journal*, April 15, 2011. *URL:*http://usma.academia.edu/PauloShakarian/Papers/708892/Stuxnet_Cyberwar_Revolution_in_Military_Affairs.

Thomas, Timothy L. (2009), “The bear went Through the Mountain: Russia Apporaches its Five –Day War in South Ossetia”, *Journal of Slavic Militrary Studies*, 22(2009):31-67.

Thomas, Timothy L (2010), “Russian Information Warfare Theory: The Consequences of August 2008”, *The Russian Military Today and Tomorrow*. URL: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=118969.

Thomas, Timothy L. (2009), “Nation-State Cyber Strategies: Examples from China and Russia”, Kramer, Franklin D.; Starr, Stuart H; Wentz, Larry (*Ed*.), *Cyberpower and National Security*, Potomac Books Inc.

Thomas, Timothy L. (2004), “Russia’s Reflexive Control Theory and the Military”, *Journal of Slavic Military Studies*, 17:237-256.

Thomas, Timothy L. (1998), “The Mind has no Firewall”, *Parameters*, Spring 1998:84-92.

Trendle, Giles (2002), “Cyber War”, *World Today*, 58(4): 7-8.

Tsyganok, Anatoly (2008), “Informational Warfare - a Geopolitical Reality”, *Strategic Culture Foundation online magazine*, November 5, 2008, *URL:*http://rbth.ru/articles/2008/11/05/051108_strategic.html.

"The Red Army Deception: the destruction of German Army Group Centre", [Online Web] Accessed 6 December 2011, URL: http://www.globalsecurity.org/military/library/report/call/call_3-88_histp.htm.

"Timeline of the events in Tallinn, Estonia", [Online Web] Accessed 8 December 2011 , URL: http://www.infoniac.com/breaking/chronology-of-the-events-in-tallinn-estonia.html.

Venkatesh, S (2003*), Cyber-Terrorism*, Delhi: Authorspress.

Vatis, Michael (2006), "The Next Battlefield: The Reality of Virtual Threats", *Harverd International Review*, 28(3): 56-.

Waltz, Edward (1998), *Information Warfare: Principles and Operations*, Artech House Publishers.

Watts, Barry D. (2011), *The Maturing Revolution in Military Affairs*, Center for Strategic and Budgetary Assessments.

Weiss, Gus W. (2007), "The Farewell Dossier: Duping the Soviets", Centre for the Study of Intelligence, Central Intelligence Agency, April 14, [Online Web] Accessed 7 December 2011 , URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm#top.