Cyber warfare: the future of war

CHAPTER I

INTRODUCTION

Karl von Clausewitz defined war as "…an act of violence intended to compel our opponent to fulfill our will In order to attain this object fully, the enemy must be disarmed, and disarmament becomes therefore the immediate object of hostilities…." At the end of the second millennium, this classification no longer describes the full spectrum of modern warfare. In the future, we will have the prospective to make war without the use of violence and fulfill the second half of von Clausewitz's definition-with software alone. Today's software intensive systems make this probable. " Cyber" describes systems that use mechanical or electronic systems to swap human control. Cyber warfare can be executed without violence and therefore the reliance on software intensive systems-cyber systems-can make nations exposed to warfare without violence.

What is Cyber? Terms with cyber used as prefix are currently in vogue not only among some visionaries and technologists seeking new concepts, but even by the man in the street, and each has its own connotation. The term cyber is from Greek root *kybernan* , meaning to steer or govern and a related word *Kybernetes* , meaning pilot, governor, and/ or helmsman. Norbert Weiner first introduced the prefix in the 1940s in his classic works creating the field of cybernetics (which is related to *cybrenetique* , an older French word meaning the art of government). Cyber, in fact has been the most acceptable term due to the reason that it bridges the gap between information and governance, the two inseparable facets of control. The prefix therefore, is freely used in the following:

1. Cyberspace . Originally coined by William Gibson in his science fiction novel Neuromancer, published in 1984, and defines it as that position within the computer where electronic activity / communication takes place. He further describes it as a place of ” unthinkable complexity”. The term has given rise to a vocabulary of “ cyberterms” such as cybercafes (cafes that sell coffee and computer time), cybermalls (online shopping services) and cyberjunkies (people addicted to being online).
2. Cybernetics. It is the science of communication and control, which interfaces a monitor (human brain or an electronic machine) to other parts of a system. The function being, to compare what is happening in the system, to what should have happened and then draw the difference, which is passed on to the control system for rectification (feedback). It applies equally to organisations, machines and organisms. Cybernetics is also used to describe a general analytical approach to control, communication and other system technologies and attempts to link engineering disciplines with the related work of social scientists through the unifying threads of feedback in its most general aspects and through its interest in transfer of information.
3. Cyberwar. A RAND Corporation synonym for information warfare, it is also sometime called netwar. Another school considers it as knowledge related conflict at the military level. However, Denis Quigley comes close by designating it as ‘ control warfare’ or leitenkreig in German. Cyberwar will be discussed more in detail later in the Study.
4. Cybernation. Loosely used, it implies digitisation of various systems of an arrangement/organisation or super systems, where electronics links

humans to machines, thereby immensly amplifying the human capabilities. It, in its most basic form, would indicate electronic automated management of information and knowledge.

Cyber warfare (CW). It is a relatively new addition to the glossary of warfare. With the escalating use of computers in military and government, there has been a growing awareness of both a new susceptibility in national infrastructure and a new method of attacking one's enemies. There is the potential of using information systems to protect, control or attack information networks. CW could mean winning wars without firing shots, the shutting down of entire national infrastructures at the push of a button, and the complete exploitation or destruction of an enemy's communication networks. It could mean threats from across the world by states with no ability to launch a conventional attack, or attacks by non-state actors using cheap laptops. There has also been talk of super-viruses shutting down nations, and how a disgruntled individual or small group could wage a ' war' on a nation. CW is the new wonder weapon, and the new unknown threat. However, the concept of CW, and the technology on which it relies, is beset by vague depictions of the dangers it presents, or the benefits it offers.

CW is conceptualised by security expert Amit Yoran, cyber-security chief at the US Department of Homeland Security and vice president of computer corporation Symantec, as the future *" primary theatre of operations"* . There is a consensus that CW is something noteworthy, but it is not clear if this consensus extends to a common understanding of what CW actually is. It is so new that there is no standard definition to describe it. This leads to one of the most frequent confusions regarding cyber warfare: its relation to

Information Warfare (IW). IW is not unproblematic in definition, but can be understood as the “ offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary’s information, information-based processes, information systems, and computer-based networks while protecting one’s own”. While IW covers the territory of cyber warfare, it also covers a much broader mandate. Electronic (‘ cyber’) communication is only one aspect of IW, which includes all information operations in a conflict. Chinese strategist Sun Tzu and Napoleonic strategist Carl von Clausewitz referred to information operations, and the importance of such operations in war. IW predates electronic communication, and is not interchangeable with cyber warfare for this reason.

CW involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks are the primary executors of these attacks. These individuals often operate under the auspices and possibly the support of nation-state actors. In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner.

Analyzing the Threat. In 2007, a denial-of-service attack was launched every 53 minutes. The 2007 FBI/Computer Security Institute study indicated that loss of revenue attributed to DDoS (dedicated denial of service) was approximately US$90, 000 an hour for a retail catalog sales company. *Malware* is a common cyber-weapon. Malware (short for malicious software)

is a computer program designed with malicious intent. This intent may be to cause annoying pop-up ads with the hope you will click on one and generate revenue, or forms of spyware, Trojans and viruses that can be used to take over your computer, steal your identity, swipe sensitive financial information or track your activities. At least five new pieces of malware emerge every two minutes, according to *Kaspersky's Internet Security Lab* . One critical measure I monitor regularly is the number of significant events reported to Hackerwatch. Org. At the time I'm writing this, in the past 24 hours, there have been more than 8 million significant incidents reported. The warning signs are there, but the question remains: Are we smart enough to prepare?

A key premise of this paper is that information processing-whether by equipment (computers) or by humans-is becoming a *" center of gravity"* in future warfare. Although there is much debate on the reality of the CW threat, the growing number of computer intrusions on government and non-government systems substantiate the fact that the threat is very real. The growing dependency on information and information based technologies have made us very vulnerable to hostile attacks Hence, our immediate goal must be to both imagine and define how foreign cyber attack capabilities might threaten information networks in India and what potential effects they might have.

METHODOLOGY

Statement of Problem

This paper seeks to study and analyse the use of cyber warfare in future conflicts & its implications on national security. To suggest India's response

to these cyber threats by outlining a clear, well defined cyber security strategy and suggest measures to safeguard own national security.

Hypothesis

As information systems permeate in military and civil lives, a new frontier is being crossed – The Information Age- which will define the future wars. Cyber Warfare has become central to the way nations fight wars and is the emerging theatre in which future conflicts are most likely to occur. Cyber warfare will take the form of a devastating weapon of the future battlefield which will be integrated in the ‘ War fighting Doctrines’ of nations across the world.

Justification of Study

The premise of cyber warfare is that nations and critical infrastructure are becoming increasingly dependent on computer networks for their operation. Also as armies around the world are transforming from a platform centric to a network centric force there is increasing reliance on networking technology. With all the advantages of such connectivity come unprecedented challenges to network security. Threats to information infrastructure could be in the form of destruction, disclosure, modification of data and/or denial of service. A hostile nation or group could exploit the vulnerabilities in poorly secured network to disrupt or shut down critical functions.

The protection of our information resources – information assurance, will thus be one of the defining challenges of national and military security in the years to come. To take advantage of Information Technology revolution and

its application as a force multiplier, the Nation and army in particular needs to focus on Cyber Security to ensure protection / defence of its information and information system assets.

Many will argue that defence and intelligence computer systems of most countries including Idia are air gapped and thus, isolated from the Internet. It may appear convincing that by air gapping the networks and using superior technology, the risk may be reduced. However, this will not provide fool proof security. With the proliferation of technology at an astronomical rate, the threat of cyber terrorism will only increase. The air gapped networks are vulnerable from insiders, disgruntled employees and moles planted or recruited by cyber terrorists or their sympathisers to cause the intended damage. A cyber terrorist may impersonate a computer technician and call individuals within the targeted organisation to obtain information to penetrate a system. Once in possession of legitimate log on information, cyber terrorists will have legal access to a system and can insert viruses, trojan horses, or worms to expand their control of the system or shut it down. In Russia, hackers used a gas company employee to plant a trojan horse which gave them control of the nation’s gas pipelines. It is against this backdrop that it becomes imperative as a soldier to understand cyberspace, the threat that it poses and to suggest some steps in order to minimise, if not eliminate the menace that it would cause.

Scope

This study concentrates on the evolution of cyber warfare and the giant leaps that it has taken in the past decade. The entire spectrum of cyber conflict, including threat reality of cyber warfare being used as a potent and

devastating weapon of the future battlefield has been covered. Further the study outlines the cyber warfare capabilities of select nations and how vulnerable India is to these threats. Finally the report outlines a cyber security strategy and recommendations for combating the cyber warfare threat in the 21st century.

Methods of Data Collection

The data has been collected through various journals, seminar papers and certain books on the subject. Some material has also been downloaded from the Internet. A bibliography of sources is appended at the end of the text.

Organisation of the Dissertation

It is proposed to study the subject under following chapters:

1. Chapter I – Introduction and Methodology.
2. Chapter II The Future of Warfare. Information Revolution and Warfare. Defining Cyberwar. Evolution of Cyber Warfare.
3. Chapter III Global Threat in Cyberspace. Threats in Cyberspae. How Real Is the Threat? Spectrum of Cyber Conflict. Recognition of the Cyber Warfare Threat.
4. Chapter IV – Combating the Threat. How Vulnerable are We? Cyber Security: A Few Initiatives. Def Cyber Warfare. Cyber security Strategy.
5. Chapter V Conclusion. The Digital Battlefield. Recommendations.

CHAPTER II

THE FUTURE OF WARFARE

“ So it is said, if you know others and know yourself, you will not be imperiled in a hundred battles; if you don’t know others, but know yourself, you will win one and lose one; if you don’t know others and don’t know yourself, you will be imperiled in every single battle.” -Sun Tzu

Will conventional warfare remain the custom for the future or will a new wave of warfare emerge? Down through the corridors of time, wars have been fought for various reasons. Conflict arose from regional instabilities, economic and social perils, and religious animosities. In their book, War and Anti-War: Survival At The Dawn of The 21st Century, Alvin and Heidi Toffler categorize the progression of warfare into three stages or waves: agrarian, industrial, and informational. While some areas of the world still remain in the agrarian realm and some others have advanced to the industrial state, a few have broken out into a completely new era-the information age.

Information Revolution and Warfare

If you know the enemy and know 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 . This extract comes from the 6th century BC Sun Tzu’s *The Art of War* and is still as compelling today as it was two and a half millennia ago. As a matter of fact, it is in all probability safe to say that knowledge and information about one’s adversary have a greater impact now than they have had at any other point in the history of warfare.

At the same time, critical information is now often stored electronically in spaces reachable from the Internet, which means there is a prospective for it to leak out to one's adversary, or for the opponent corrupting it in order to affect one's decision making capabilities.

There is no standardised definition of Information Warfare. However it has been defined as " Actions taken to achieve information superiority by affecting adversely information, information based processes, information systems and computer based networks of the adversary, while protecting one's own information".

An aim of warfare always has been to affect the enemy's information systems. In the broadest sense, information systems encompass every means by which an adversary arrives at knowledge or beliefs. A narrower view maintains that information systems are the means by which an adversary exercises control over, and direction of fielded forces. Taken together, information systems are a comprehensive set of the knowledge, beliefs, and the decision making processes and systems of the adversary. The outcome sought by information attacks at every level is for the enemy to receive sufficient messages that convince him to stop fighting.

Information Warfare is a form of conflict that attacks information system directly as a means to attack adversary's knowledge or beliefs. Information Warfare can be prosecuted as a component of a larger and more comprehensive set of hostile activities a net war or cyber war or it can be undertaken as the sole form of hostile activities. Most weapons, a word used to describe the lethal and nonlethal tools of warfare only have high utility

against external adversaries. While most often employed against external adversaries, many of the weapons of information warfare are equally well suited for employment against internal constituencies. For example, a state or group cannot use guns or bombs against its own members; however, the weapons of Information Warfare can be used, have been used, and very likely will be used against both external and internal adversaries.

Information warfare as defined by Martin Libicki has seven components:

1. Command and Control Warfare.
2. Intelligence based warfare.
3. Electronic Warfare.
4. Psychological Operations.
5. Hacker Warfare.
6. Economic Information Warfare.
7. Cyber Warfare.

This concept of seven components is universally recognised today, as it encompasses the entire spectrum that Information Warfare offers. Besides, it strongly argues that Information Warfare is not exclusively a military function and various actors viz. the media, private industry and civil society including civilian hackers play a key role in building a nation’s capability to wage Information Warfare. The role of private industry has gradually been acknowledged as cutting edge information technologies become increasingly pervasive in sensors and weapon systems. The information systems while making the military more efficient also render it vulnerable to attacks on the systems itself. Winn Schwartau, also known as the “ Civil Architect of

Information Warfare" has defined Information Warfare in this very context: " Information Warfare is a conflict in which information and information systems act as both the weapons and the targets". As far as the Indian viewpoint on Information Warfare is concerned, history amply reveals that information was essentially viewed as a strategic resource. Kautilya, the great strategist of the Maurya period, strongly advocated the need of obtaining accurate information about the enemy forces and plans of action. In fact, he is considered to be instrumental in the victory of the Mauryan's and placing Chandragupta Maurya on the Magadha throne. His astute thinking on warfare and statecraft is portrayed in the famous treatise Arthshastra. While postulating that war may not always be the right option, Kautilya espoused the importance of information and knowledge in winning wars.

Information Superiority and Cyber Warfare . Information Technology is a double edged weapon. It provides vast opportunities but simultaneously introduces new vulnerabilities and threats, which may arise through computers, content and connectivity or, to put it differently, hardware, software, information and networks. Information superiority over our adversaries including militant and terrorist outfits is very essential. Non Lethal information weapons can black out communication systems, destroy valuable data and cripple the nation. Therefore, we have to act faster than any adversary. This requires defensive as well as offensive cyber warfare capabilities. Cyber warfare can be a full fledged war and vital infrastructure shall get targeted. To handle cyber wars, highest national level decision making is required, in real time and with full fall back options. For this

purpose, basic building blocks include excellent monitoring tools for network traffic, web sites and databases, intrusion detection, firewalls, encryption and decryption algorithms, public key infrastructure and remote access facilities. Offensive cyber warfare spans computer crimes and information terrorism. Everyone is under threat telephone, power supply, banks, transport, and the day to day needs. lt is important to create tools, awareness, and structures to assess threats to information resources, including military and economic espionage computer break-ins, denial-of-service, destruction and modification of data, distortion of information, forgery, control and disruption of information flow, electronic bombs, etc. ln essence, the thrust of the initiatives must lead to information assurance like life assurance.

Defining Cyberwar

Cyber Warfare. It is the sub-set of information warfare that involves actions taken within the cyber world. There are many cyber worlds, but the one most appropriate to cyber warfare is the Internet and related networks that share media with the Internet. Cyber Warfare as related to defence forces refers to conducting of military operations according to information related doctrine. It means disrupting or destroying information databases and communication systems. It means trying to know everything about the enemy while keeping the adversary from knowing much about oneself. It means turning the equilibrium of information and knowledge in one’s favour especially if the balance of forces is not. It means using information so that less capital and labour may have to be expended.

Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related ideology. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to “ know” itself: who it is, where it is, what it can do when, why it is combating, which threats to counter first, etc. It means trying to know all about an opponent while keeping it from knowing much about oneself. It means turning the “ balance of information and knowledge” in one’s favour. This form of warfare may involve diverse technologies-notably for C3I; for intelligence collection, processing, and distribution; for tactical communications, positioning, and identification-friend-or-foe (IFF); and for “ smart” weapons systems-to give but a few examples. It may also involve electronically blinding, jamming, deceiving, overloading, and intruding into an adversary’s information and communications circuits. Yet cyberwar is not simply a set of measures based on technology. And it should not be confused with past meanings of computerized, automated, robotic, or electronic warfare.

Cyber warfare requires different principles of warfare which have been derived from thousands of years of experience as documented by Sun Tzu, Clausewitz, Jomini, Liddell-Hart, and others. Some of the kinetic warfare principles apply to cyber warfare while some principles of kinetic warfare have no meaning in cyber warfare. Some principles of kinetic warfare may actually be antagonistic to cyber warfare. The various characteristics and principles of cyber warfare are as under:

1. Waging cyber war is relatively cheap. Unlike traditional weapon technologies, acquiring information weapons does not require vast financial resources or state sponsorship.
2. Boundaries are blurred in cyberspace. Traditional distinctions public versus private interests, warlike versus criminal behavior, geographic boundaries, such as those between nations tend to get lost in the chaotic and rapidly expanding world of cyberspace.
3. Opportunities abound to manipulate perception in cyberspace. Political action groups and other nongovernment organisation’s can utilize the Internet to galvanize political support.
4. Cyber war has no front line. Current trends suggest that the economy will increasingly rely on complex, interconnected network control systems for such necessities as oil and gas pipelines, electric grids, etc. and these will become vulnerable to cyber attacks.
5. Cyber-warfare must have kinetic world effects. Cyber warfare is meaningless unless it affects someone or something in the non cyber world.
6. Anonymity. Cyber warfare can be waged anonymously. Anonymity is the nature of new technologies, especially telecommunications. An anonymous attack creates two problems. Not only has a state’s national security been breached, but there is no one to hold accountable for the attack.
7. Offensive Nature. Information technology and computer systems are vulnerable by nature. Therefore, taking defensive measures against the information warfare threat will always be difficult and costly. Improving the defense of information systems also contributes to the

security dilemma since decreasing one’s susceptibility to information warfare increases the attraction of using information warfare offensively.

Cyberwar may have broad ramifications for military organization and doctrine. As noted, the literature on the information revolution calls for organizational innovations so that different parts of an institution function like interconnected networks rather than separate hierarchies. Thus cyberwar may imply some institutional redesign for a military in both intra- and inter-service areas. Moving to networked structures may require some decentralization of command and control, which may well be resisted in light of earlier views that the new technology would provide greater central control of military operations. But decentralization is only part of the picture; the new technology may also provide greater “ topsight”-a central understanding of the big picture that enhances the management of complexity. Many treatments of organizational redesign laud decentralization; yet decentralization alone is not the key issue. The pairing of decentralization with topsight brings the real gains.

Cyberwar may also imply developing new doctrines about what kinds of forces are needed, where and how to deploy them, and what and how to strike on the enemy’s side. How and where to position what kinds of computers and related sensors, networks, databases, etc. may become as important as the question used to be for the deployment of bombers and their support functions. Cyberwar may also have implications for the integration of the political and psychological with the military aspects of warfare.

In sum, cyberwar may raise broad issues of military organization and doctrine, as well as strategy, tactics, and weapons design. It may be applicable in low- and high-intensity conflicts, in conventional and non-conventional environments, and for defensive or offensive purposes.

As an innovation in warfare, I anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century. At a minimum, it represents an extension of the traditional importance of obtaining information in war-of having superior C3I, and of trying to locate, read, surprise, and deceive the enemy before he does the same to you. That remains important no matter what overall strategy is pursued. In this sense, the concept means that information-related factors are more important than ever due to new technologies

Evolution of Cyber Warfare

Since the early days of the Internet, there were individuals trying to compromise computer systems' security via the network. Initially their activities were limited to defacement of web pages and motivated mostly by mere thrill seeking. In the 1990's political activists realized the potential for publicity coming with the attacks, and defacements carrying a political message became more frequent (Hacktivism). The palette of attack types also widened greatly, most notably some of them became aimed at bringing services or whole systems down, by generating excessive network traffic (denial of service, email bombardments).

The first reported politically motivated cyber terrorist attack using a flood of emails was carried out by the Tamil Tigers against Sri Lankan embassies in

1998. It was successful, even as it did not bring targeted servers down, because more importantly it attracted worldwide media attention to the attackers' cause. Activist groups involved in other struggles around the world soon followed with similar attempts.

The diplomatic conflict between Pakistan and India over Kashmir has, since the late 1990's, been paralleled by a series of mutual cyber attacks. In the Middle East, every time political or military fight escalated between Israel and Palestinians, so did fights on the virtual battlefield. Both sides have used sophisticated techniques and well planned strategies for their cyber attacks. Pro-Palestinian attacks have been carried out by a number of terrorist groups (some of which even came up with the term cyber jihad), and pro-Jewish ones might have been coordinated by the state of Israel, though there is no clear evidence to support that. Studies have shown that Israel leads the list of countries in terms of numbers of conducted computer attacks per 10, 000 Internet users.

This brings us to the newest trend in cyber warfare: cyber attacks carried out by hacker groups inspired, coordinated, funded and supplied with resources by nation states. They are usually large scale and prolonged operations targeting specific systems within enemy structures. Probably the first of this type of attacks took place during the NATO air strikes against targets in Former Republic of Yugoslavia during the Kosovo violence in 2000. Targeted were all 100 of NATO servers, each subject to excessive network traffic originating mostly from Serbia, as well as Russia and China – it's supporters in the conflict. The cyber attacks caused serious disruptions in NATO's

communication and services, lasting several days, but did not directly affect the bombing campaign.

These days cyber warfare still mostly consists of uncoordinated cyber terrorism acts performed by groups whose main aim is publicity and media coverage. Gradually though the nature of cyber warfare is going to change into activities coordinated and paid for by nation states and large international terrorist networks. We can expect attacks trying to exploit vulnerabilities in critical infrastructure like telecommunication systems, airports, power plants, oil and gas infrastructure, supply of water, and military systems. In the coming years we are likely to see a quick rise in the number of cyber battles and one can imagine that in the future wars are going to be fought without dropping bombs and firing missiles.

CHAPTER III

GLOBAL THREAT IN CYBERSPACE

Threats in cyberspace

There are four fundamental categories of threats to our information and information infrastructure, characterised by the degree of structure in their attack capability and the measure of trust or access that the threat enjoys. These categories are:

1. Unstructured External Threats. These are individual or small group of attackers who rely heavily on other's tools and published vulnerabilities. They attack targets of opportunity and lack persistence against difficult targets.

2. Structured External Threats. These are coordinated attackers i. e. hostile intelligence agencies or organised crime syndicates, which possess a deep technical knowledge of the target, strong motivation, and the capability to mount combination attacks using multiple complex tactics and techniques.
3. Non Malicious Internal Threats. These are accidental breaches of security caused due to ignorance or malfunctioning of system.
4. Malicious Internal Threats. Here the attackers are trusted members of the org or a less trusted support worker with some degree of access.

The threats can also be classified under the following heads: