International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Information Warfare - It's Impact on Future War and Options for Bangladesh

Md. Mostafizur Rahman

Army IT Suppout Organization, Dhaka, Bangladesh

ABSTRACT

We are now at the dawn of a new age of "Information Revolution", which is changing the concept of state's security and the art of waging war. With the creation of Information Technology (IT), the concept of Information Warfare (IW) has come into existence. The development of IT has given warfare a new dimension. Whoever controls or dominates the information-sphere will have the power to dominate the future battlefield. Since, Bangladesh is on the threshold of development in IT sector, it is now appropriate to comprehend the subject with regard to ascertain the impact of information warfare on the national security and explores the probable options for Bangladesh. Finally, practicable recommendations have been made for the implementation of information technology addressing the future challenges for Bangladesh.

INTRODUCTION

1. We live in an age that is driven by information. The society has undergone a change with the boom in the field of information technology (IT). This has extensive implications on the governance and security of a nation in peace as well as war, indeed civil and military responsibilities with this regard is nearly equal. The information age has therefore blurred the dividing line between the civil and military information agencies. Carl Von Clausewitz realized the importance of information in war saying, "the word 'information' denotes all the knowledge of the enemy and his country; therefore, in fact, the foundation of all our ideas and actions". Information in warfare has great value and hence should be recognized as a national and military asset.

2. With the revolution in the field of IT all over the world, the art of warfare has entered yet another realm – The realm of Information Warfare (IW). IW is simply the directed value of information to achieve national objectives. It has become the key factor for national power and vital national resource for the development of a nation. IW has neither boundaries nor limits. The introduction of IT has widened the scope of military leaders to conduct the war in a more conducive manner. With the control and dominance of information, the techniques and utility of IW has become main focus now.

3. IW is the emerging theatre in which future wars will occur in the strategic level and this will be superimposed on the conventional conflict. The IW has the capability to act as a super force multiplier to alter conventional superiority and gaining absolute information dominance. Armed forces in future battlefields have to keep abreast with the latest advancement in the field of IT if it has to win a future war, since the side that has superiority on information can only change the outcome. Such a conflict at the information level will permeate each fabric of the society, which depends on information. The moot question is how the society and the nation as a whole adapt to such situations.

4. Bangladesh, an economically poor country remains vulnerable to others due to her technological lag. In this context she needs to improve her IT and adopt IW to a reasonable extent. This will not only keep her in a same footing with others but also will enable her to fight a war conducive to her own requirement. The rise of computer and information use in the national affairs including security is dramatic. Its potential is worth reckoning but what comes along with this advancement is the threat of being vulnerable to IW.

DEFINATION AND LEVELS OF IW

5. The working dictionary of the National Defence University's School of IW and Strategy defines the IW as, "Action taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information systems and in the process achieving an information advantage in the application of force. It is also actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems.

Levels of IW

6. The tools to wage IW are available to anyone with an agenda and attitude. It can be conducted at three distinct levels of intensity, each with its own goals, methods and targets:

(a) **Class 1: Personal IW**. This class of IW describes attacks against an individual's electronic privacy. It is targeted at individuals, and involves accessing, manipulating, or even destroying the data concerning that individual which is held in computers and databases entries wherever information is stored.

(b) **Class 2: Corporate IW**. It is carried out against companies and organisations, and can involve techniques of class 1 IW plus other industrial espionage technologies such as intercepting the stray electromagnetic radiation from computers and Fax.

(c) **Class 3: Global IW**. On the global level, IW can be waged against industries, economies, nations or non-state groups. It ranges from intelligence and information and leads to the terrifying possibilities of terrorist groups breaking into communication such as air traffic control system.

FORMS AND FEATURE OF IW

Forms of IW

7. To say that IW is a separate technique of war is debatable. It does not exist as a separate technique of waging war, but it integrates and multiplies with war effort. Information is both a force multiplier and recourse multiplier. Dr. Martin Libick of National Defence University, USA, is of the view that there are basically seven forms of warfare which fall under the umbrella of IW. These are discussed below:

a. **Command and Control Warfare**. Command and Control Warfare aims at implementing IW on the battlefield and integrates physical destruction. Its objective is to target and physically destroy the enemy's command and control centre.

b. **Intelligence-Based Warfare (IBW)**. IBW occurs when intelligence is fed directly into operations to bring transparency of the battlefield rather than being used as an input for overall Command and Control. IBW is the direct application of battlefield intelligence instantaneously into the battle.

c. **Electronic Warfare (EW).** EW is specific mainly to military operations with the aim of dominating the electromagnetic spectrum i.e. it will aim at electronic disruption of enemy's communication systems and sensors.

d. **Economic IW**. Economic IW affects each other's economy. It has got two forms: namely, 'Information Blockade' and 'Information Imperialism'. The aim is to impose information blockade presuming that well being of societies will be as affected by information flow as by flow of material supplies. The second one implies to someone's complete information superiority or dominance over others.

e. **Cyber Warfare**. Cyber-Warfare represents the remaining possible elements of IW that may or may not be realistic at present. It includes information terrorism.

f. **Psychological Warfare**. Psychological warfare encompasses the use of information against the human mind rather than against computer support.

g. **Hacker Warfare**. Hacker warfare aims at attacking enemy's computer system. Hacking is the technique of gaining unauthorized entry into a targeted computer network.

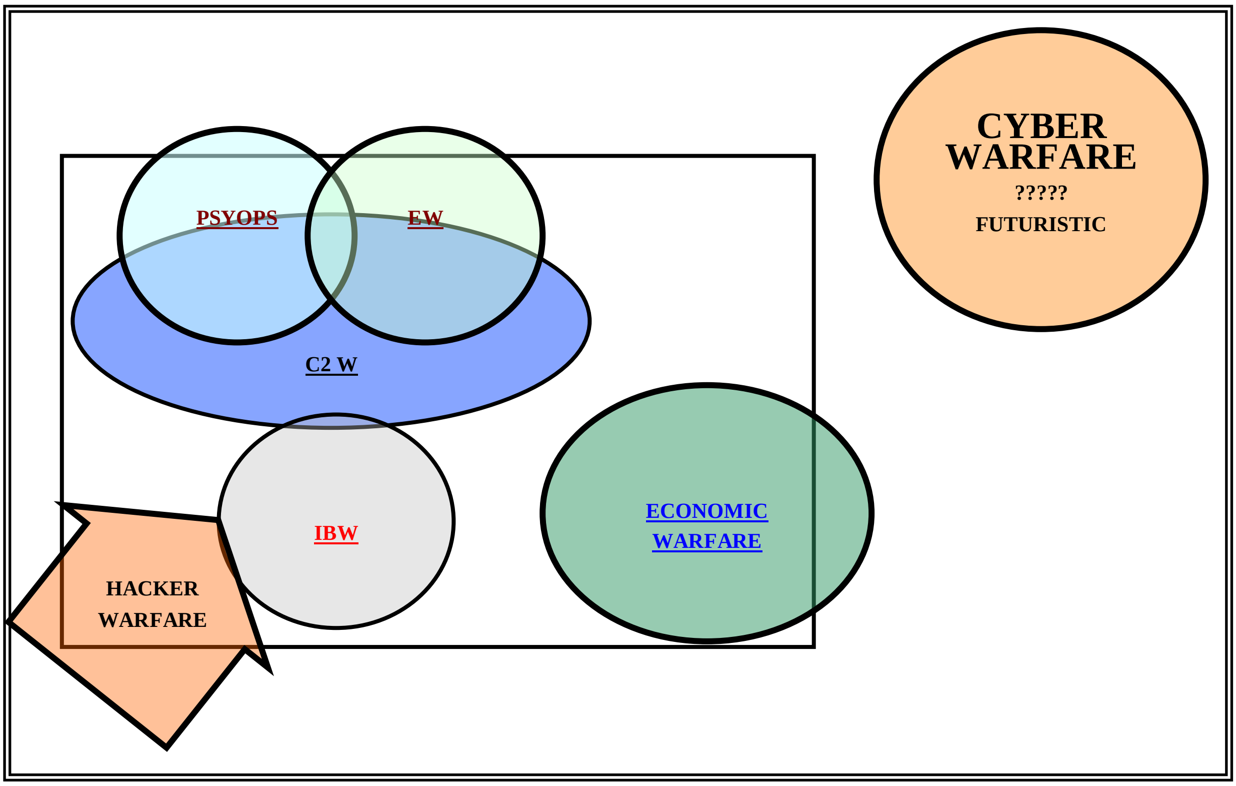

Figure 1. Forms of IW

METHODS / TOOLS OF IW

8. The methods of IW can be broadly divided into Software, Hardware and Electronic Tools. However there are few other methods as well. The common methods by which IW is conducted are explained below:

9. **Software**. Software is less than perfect and thus is one of the most sensitive pieces of the computer system, making it most vulnerable to attack. This is achieved by the following ways and means:

a. **Sniffing**. Sniffing is basically listening to conversations between computers over networks. There are two types of sniffing: active and passive. For active sniffing information warrior can tap into the network on any wire that carries network data.

b. **Computer Viruses**. It is a program which has the ability to propagate itself and infect other programs. With this feature, it can eat up files or source software, storage space, etc., whatever the designer wants. Massive failures can be caused with a virus.

c. **Worms**. A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Worm can cause the loss of communication by eating up resources and spreading through the networks.

d. **Trojan Horses**. A Trojan horse is a code fragment that hides inside a program and performs a disguised function. A Trojan horse could be camouflaged as a security related tool for example Security Administrating Tool.

e. **Trap Doors**. A trap door or a back door is a mechanism that is built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system circumventing normal system protection.

10. **Hardware**.

a. **Chipping**. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions.

b. **Nano Machines and Microbes**. These are small robots which can crawl into halls and offices and enter the computer through the holes in the cover and shut down the electrical circuit in the computer or damage them severely. Special breed of microbes that eat silicon chips can also be used.

11. **Electromagnetic Means**.

a. **Electronic Jamming**. From the old days electronic jamming was used to block communication channels at the enemy's equipment so that they can not receive any information. The next step is not to block their traffic but instead overwhelm them with incorrect information.

b. **High Energy Radio Frequency (HERF) Guns**. HERF Guns shoot a high power radio signal at an electronic target and put it out of action by overloading sensitive circuits with energy.

c. **Electromagnetic Pulse Transformer (EMPT) Bombs**. EMPT bomb is essentially the same as a HERF gun but a thousand times more powerful. The source can be nuclear or non-nuclear detonation. It destroys the electronics of all computer and communication systems in a large area.

IW : IMPACT AND CONCERNS ON WARS

Impact of IW

12. IW has changed the way we think (doctrine), organise and fight. At the same time IW has made the battlefield smaller, but it has vastly increased the potential scope of battle and the tempo of the battlefield operations. The impact of IW stretches to all centres of power without any boundaries or limitations. The close link of media and IT and extensive use of IT in media has generated a new era of IW. Realm of the IW impact is shown in figure 2 as block diagram.

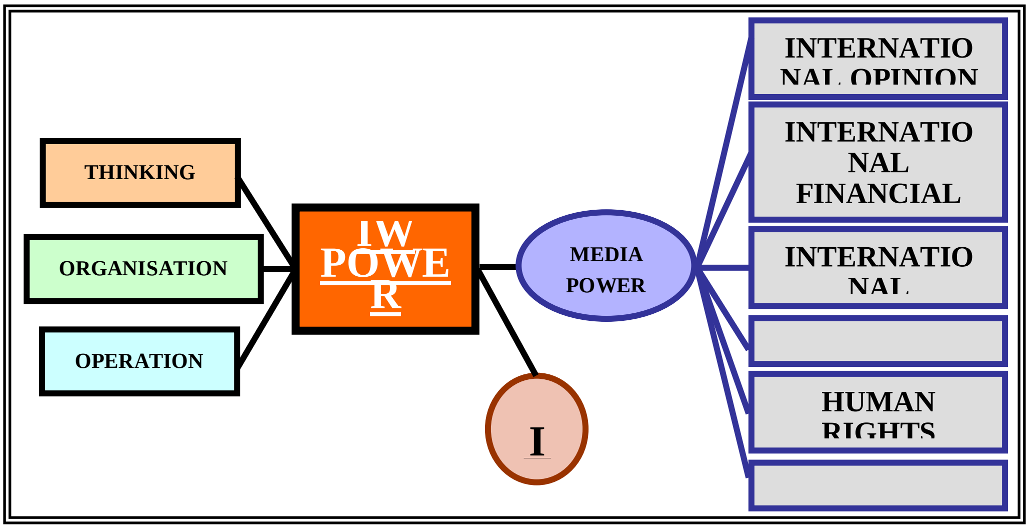

Figure 2. Realm of the IW Impact

Impact of IW on Recent Wars

13. **Gulf War**. The Gulf war was the first time when information was used both as a target and as a weapon[1]. Command and Control (C2) centres, communication facilities, TV and radio stations were the first to be struck with missiles and bombs. In the initial stages, the Iraqi units were cut off from their command echelons. In which allied forces destroyed the C2 set up of Iraq. The precision weapons were used basing on data from information technology and stroked on pinpoint.

14. **Kosovo War**. From the outset of Kosovo conflict in 1999, NATO used its IW assets to shut down Serb computers used in command and control of air defence network. In one occasion, the Pentagon considered hacking into Serbian computer networks to disrupt military operations and basic civilian services. But it refrained from doing so because of continuing uncertainties and limitations on the emerging field of cyber warfare. This was done with the belief that, the computer system control communications, transportation and other services in a foreign country may not only impact military operations but have the cascading effect of disrupting civilian life as well.

15. **Operation Iraqi Freedom**. In Operation Iraqi freedom 2003, USA launched the first strike 90 minutes after President

Bush's 48 hours dead line to Saddam and his sons to leave Baghdad expired at 8 P.M (GMT 0100) 20 March 2003. Two F-117A stealth fighters dropped precision guided 2000 pound bombs and nearly 40 Tomahawk cruise missile launched from the ship stationed in the Red Sea. The targets were precisely identified and locked. Through satellite image large movement of troops including move of small vehicle were identified and destroyed. Iraqi command echelon was completely jammed and destroyed by exclusive use of information technology. The coalition forces used all modern computer based technology and tried to prevent innocent civilian causality.

SIGNIFICANCE OF IW FOR BANGLADESH

General Perception

16. Significant changes in information age have definitely warranted all the nations to have formidable mechanism of protecting NII which other wise calls for development of IW. But in the case of Bangladesh a common misconception is prevailing that IW does not have relevance for Bangladesh as it is argued that Bangladesh is relatively 'low-Tech' and less computerised. As such, she has little to loose from information attacks. But Bangladesh has already on the verge of threats from IW and it has significant number of assets that are to be protected from enemy information attacks. Hence we need to give due emphasis on the subject to evaluate our vulnerabilities for our defence.

IW and Bangladesh

17. Information Revolution for a country like Bangladesh seemed a long time in coming. But, in fact, change has been insinuating itself into the daily lives all along. In Bangladesh, 53 per cent of the computer use has started after 1995. A giant step in making the Information Revolution real for the masses has been the lifting of taxes from the computers by the government in 1998 and commercialization of the Internet, the vast skein of computer networks that provides access to virtually limitless stores of information around the globe. Present Information Technology has already started to change the age-old systems in Bangladesh. Figure 3 shows the present percentage of computers usage for office automation in different sectors. By 2020, activities involving the operation and control of essential physical and functional infrastructures--power grids, air traffic control systems, telecommunications and the like - will be shifted from mechanical/electrical control to electronic/software control.

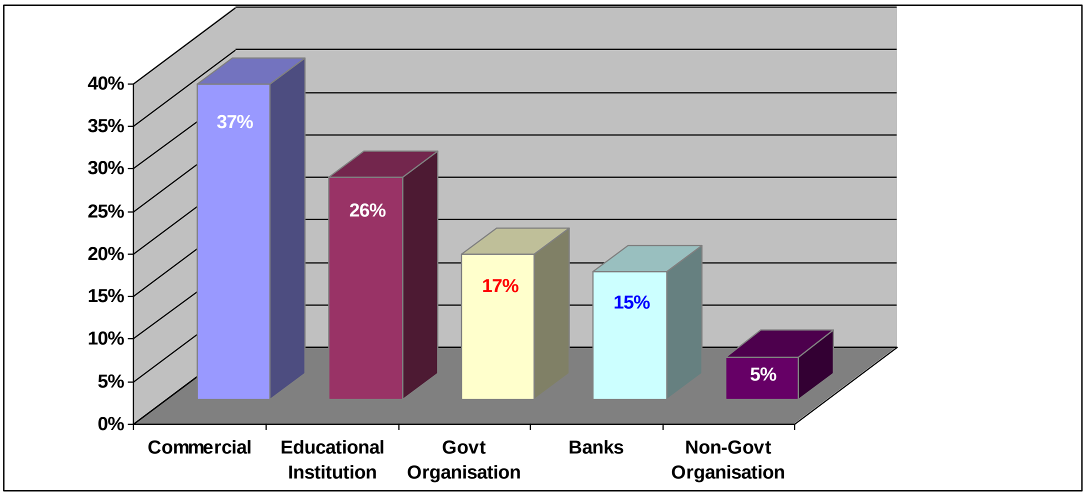

Figure 3. Sectors of Office Automation in Bangladesh

Elusive Bottom Line of Threat for Bangladesh

18. After the war of liberation in 1971, Bangladesh did not face any general war or limited war. Besides the counter insurgency operation at Chittagong Hill Tracts, the government machinery and the normal life of the people are often disturbed by the terrorist activities in Bangladesh. In the present IW scenario, it is presumed that tomorrow's terrorist may be an information terrorist. To act, terrorists need not to man the "line of control" or "international boundary". Many existing information systems do appear to be vulnerable to 3some level of disruption or misuse. More so, with the proliferation of IT, the threat to national security will also rise. Whatever systems are operating in Bangladesh is now poorly protected, few intrusions are detected and very few of those detected are actually reported. In fact, there is no awareness on the vulnerability of the present systems and far too less on the concept of IW in the IT industry of Bangladesh.

19. Knowing the basic features as well as future threat scenario careful attention needs to be given to the possible solidifying of a bottom line on the gravity of the cyberspace-based strategic IW threat. The targets for future war or conflict will be information system and computer network in the field of command, commerce and media that can paralyse the nation. We know that our most potential adversary is aided and abetted by advanced technology and capable of springing any kind of surprise. We cannot afford to be on the sidelines in this regard and it is but imperative that we gear ourselves solidly to face this new realm of warfare. Therefore, it is essential to comprehend the nature and characteristics of information or cyber wars that Bangladesh is likely to face in future. This should be the first step for Bangladesh towards evolving a strategy to base own doctrine, organisation and training.

POSSIBLE OPTIONS FOR BANGLADESH TO COUNTER IW

IW Counter Measures

20. Effective counter measures against IW include both deterrence and system defensive measures. Following are some of the common and accepted system defences:

a. **Systems Vulnerability Analysis**. Systems vulnerability analysis and improved design can yield three positive results. Besides the obvious result of reducing vulnerability, the systems can be made less attractive targets; that is, successful attacks would yield less damage and publicity.

b. **Systems Hardening**. Hardening and protective measures should be designed into all systems. This is an enormous field that spans the spectrum from satellite antenna design to electrical protection of personal computers and workstations.

c. **Security Training**. Security training is absolutely essential at all levels and without it other defensive measures are less effective. Password protection, for example, can make information systems less accessible, but bad procedures can defeat its purpose.

d. **Redundancy and Backup**. Redundancy and backup methods reduce or limit the harmful effects of an attack or system penetration. Frequent backup can minimize the damage caused by lost, stolen, or disrupted data, and information can be rapidly restored or reconstituted.

e. **Aggressive Law Enforcement**. Aggressive domestic and international law enforcement can certainly have a deterrent effect on potential adversaries. Since cyberspace recognizes no borders, international agreements and laws are necessary.

CONCLUSION

21. With the proliferation and development of IT, the recent concept of IW has developed. IW is not new, but the rapid technological advances in information systems have vastly increased the value of information in warfare. Hence, Information in warfare should be recognised as a military and national asset. The concept of IW covers a wide range of issues. In essence, IW deals with offensive and defensive use of information and INFOSYS to deny, exploit, corrupt or destroy an adversary's information systems vis-à-vis protecting own one's. That means, measures to be taken to achieve information superiority by affecting adversary's information environment while own information system to be defended.

22. It is very difficult to anticipate the future field of warfare. Rapid and vast development of technology vis-à-vis weaponry system made the future battlefield critical and confusing. Thereby it is predicted that in future, IW will destroy the enemy's will to fight, primarily dealing with C3I with vast technological advancement. It is obvious that in future, information may appear as weapon rather than a tool that are supporting traditional kinetic weapons through information data. Thereby we may imagine that the trends of war in future likely to be violent military and non-violent wars. These will have similar types of combat but of greater magnitude.

23. Bangladesh is one of the Least Developed Countries of the world, yet it is moving fast towards computerization and networking of the society. At present Bangladesh is not in the list of highly vulnerable countries with regard to IW. The banking, telecommunication, education, air communication and business sectors of Bangladesh are increasingly adopting technological advantage. It is expected that with in next few years, Bangladesh would get most of the service sectors computerized. The more a nation gets digitized and automated, the more vulnerable it becomes to information attacks. Thus, the future networked society would increase the vulnerabilities to this type of warfare in the years to come. Vital national economic, information infrastructures, and national psyche now assume greater significance in the context of overall national security perspective.

RECOMMENDATIONS

24. From the above study on IW, following steps are recommended to develop an effective IW capability for Bangladesh in the coming years:

a. Immediate steps should be taken to create awareness of IW among all the IT users, service providers and Defence Forces through seminars, discussions and formal security training.

b. Government should immediately formulate a National IW Committee to carry out periodic system vulnerability analysis and recommend effective defensive measures. The government should also formulate a national IW strategy and IW doctrine that will outline the role of all the user agencies susceptible to IW threat.

c. To face the challenge of 21st century Bangladesh government should restructure her Armed forces in accordance with the perceived IW threat for Bangladesh. In this regard, to find out the exact state of C4I and decision making process in the Armed Forces, a separate IW directorate may be incorporated in the existing organisation of the services HQ and IW wing may be established in the AFD for tri-services co-ordination.

d. A sound plan needs to be developed at the national level for monitoring and effective protection of cyberspace wherever it affects our national interest.

e. Training issues like more IT awareness at military training schools and centres may be implemented. Various civil and military courses may be conducted customizing and covering all aspects of IW.