DIMENSIONS OF CYBER WARFARE IN INDIA

Divya Dwivedi
Senior Research Scholar, Defence & Strategic Studies, University of Allahabad, India.
Email - deeds.dwivedi@gmail.com

Abstract: *This paper gives a close look to the very important aspect of National security in today's world of globalization and information cyber security. The role of social media, cyber security, hacking and cyber terrorism are dealt in the paper with special reference to India. All dimensions of cyber security in India are mentioned with examples from last few years' incidences of cyber warfare and hacking. We are witnessing a worldwide technological boom, wherein highly sensitive Government data to minute details of everyday life is digitally handled. Modern warriors, also known as hackers have the ability to hack into computer systems that can collapse networks and cause both human and infrastructural loss.*

This paper shows different aspects of cyber security in India, its objective, functions, threats, challenges etc. and finally conclusion. At present time in India, the development of cyber-assets depend upon how strong protection measure we have devised to protect it. It is the stage when cyber security should be placed at the zenith of priority even if it amounts to certain modifications and alterations in India's cyber domain. If the cyber security of the country is to be preserved the most pertinent consideration is that the security measures must be devised keeping in mind the native conditions and shall be developed by the Indian minds. This consideration again remind us the reason behind formal division of roles and responsibilities between the civil and military functions of cyber security.

Key Words: *Cyber warfare, India's National Security, Cyber-attacks, Cyber Security, Hacking.*

1.INTRODUCTION:

Nature of warfare is undergoing rapid change along with the changing geopolitical situation. Its evident that world is unlikely to see large scale conventional wars as in the past, primarily because of the increasing number of nuclear armed powers and the resultant threat they pose of escalating a war into a nuclear holocaust. With increased incidents of local insurgency and terrorism, future conflict is more likely to be limited and asymmetric in nature. Modernisation of the army is a incessant process and needs to be directed towards acquiring a desired capability, which will majorly depend on the analysis of threats. Though Pakistan will continue to remain an adversary in the foreseeable future, our major concern should be China. Its pertinent that the army now requires to base its capability building catering to this larger threat, which would inadvertently take adequate care of the threat from our traditional adversary too.

Its important for the army to transform to a light-lethal-wired force to be able to face the challenges of modern warfare. This would necessitate, among other things, the acquisition of a range of sophisticated devices, networked and capable of providing 24x7 surveillance and communications, operating in a hostile electromagnetic environment. Next generation mobile weapon platforms would be required with larger stand-off distances, precision guidance and higher lethality. Also, its important for the army to have the requisite capability of degrading similar systems and platforms of the enemy. Organizational and process changes are necessary for optimizing the deployment of existing combat and logistic resources.[1]

This is the information age and therefore like all lucrative assets of the past ages, information assets must be an object of competition and conflict – and in extreme cases, warfare. This conflict is being played out in a new domain: the cyber-space. With increasing dependency on the cyber domain for every aspect of human endeavors, it is obvious that like all national assets, India's cyber-space has to be secured against all forms of espionage, subversion, sabotage and attack.[2]

Cyber-attacks pose more than a theoretical challenge to the Indian government's day-to-day national security agenda due to the intrusions and web defacements experienced after New Delhi's nuclear weapons test and in the confrontation with Pakistan over Kashmir. The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations.

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through soloed ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialised has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as an NW (network) created by academics for the use of the military, it has now become a global social and economic and communications platform.[3]

2. DEFINING CYBER WARFARE:

There is as such no agreed definition of cyber warfare but it has been generally contemplated as states attacking the information systems of other countries for espionage and for disrupting their critical infrastructure. Mainly, it refers to politically motivated hacking to conduct sabotage and espionage. Analogy of this form of information warfare is generally drawn to conventional warfare although controversial for both its accuracy and its political motivation.[4]

To have a better understanding of the nomenclature Cyber Warfare it can be said that they are offensive as well as defensive information operations unleashed to have Information Superiority over the other. Unlike conventional Information Operation being carried over physical domain, in Cyber Warfare electro-magnetic spectrum or electronic domain is used for the Information Operations.

Cyber warfare is double sided sword and it can be used to disrupt the civil amenities and can target the adversary's economic and administrative infrastructure however on the other end it can be an endeavor to disrupt or hamper the information-based Command, Control, Communication, Co-ordination, Intelligence and Inter-Operable Systems (C4I2) and thus it can be strictly termed as military operation of war and ought to be dealt in a way military operation are being dealt with.[5]

3. OBJECTIVES:

The purpose of Cyber Warfare is to undertake defensive and offensive Operations in the cyber-space to degrade enemy's early warning, data analysis, intelligence exchange, decision support, and command, control and communication network. In short, the entire system of military net-centricity. At the same time protecting own information assets from hostile net centric attacks.. In offensive operations, that goal is achieved by making inroads into the enemy's digitised information that circulate in the cyber-space. However, in defensive mode, besides adoption of general security measures, the effort cannot be so much in locking up own volumes of information in the cyber domain that is impractical to achieve. The effort therefore is to identify the processes of the adversary's offensive Information Operations and neutralise these through corresponding counter-offensive measures.

Objective of Cyber Warfare is to protect own networks while disrupting that of the enemy and this is achieved by gaining information superiority in the aspects of surveillance , data analysis, intelligence exchange, command and control of battle elements and flow of communication.[6]

4. FUNCTIONS:

There are five domains in which the civil as well as military functions of national security have to be performed, viz, land, sea, air, space and cyber- space. In reference to the last named, it is a common supposition that there is singular convergence of civil and military functions. The misconception is reflected in the use of undefined terminologies and loose semantics which lead to confusing juxtaposition of concepts that govern the issue of cyber security. Factually though, the said convergence is no more prominent than it is in the context of civil-military interplay in all of the other domains of inter-state competition and conflict. In order to make the best use of our resources in achieving a fair degree of cyber security therefore, it is important to promote clarity and consistency in ruling definitions and concepts in the Indian context.

It's important to understand that every nation nurtures its own set of specific aspirations in consonance with a given set of geo-political, social and natural assets. These aspirations pave way for national prosperity, which must be protected by the triumvirate of national power, viz, socio-political, economic and military security. The first two of these aspects of security are civil functions whereas the third takes recourse to warfare to perform its role. The distinction to note here is that the civil functions of socio-political and economic security of a nation is bound by inter-state ideological differences, geo-political adversities, competition for resources and business rivalries - all aimed at extracting more and more self-advantages. This is a continuous process. Military security, on the other hand, is an extreme step that is performed as a last resort to force the adversary to desist from his unbearable animosity either by threatening to, or by actually inflicting physical punishment on him. For the intervening periods of no-war, the purpose of the military institution is to prepare for that extreme eventuality called 'war'. This distinction between the civil and military functions of national security influences the domain of the cyber-space just as it does in others domains of competition and conflict; it has universal applicability.

In the Indian context appreciation of the afore-stated distinction is more relevant. This is so because unlike America or China and a host of other countries, in the Indian dispensation, military power is not seen as a fulcrum of nationhood. Recognition of the distinction would obviate emergence of discrepancies between the civil and military functions that is caused by use of undefined phraseology like 'cyber security', 'cyber-attack', 'cyber warfare' etc.; our cyber policies must clearly convey as to what is intended to be accomplished.

Civil Functions of Cyber Security

Civil functions over the cyber-space have four denominators: -

- Public Services (health, education, civil-supplies, social security schemes, essential services),
- Financial Services (banking, subsidy funding),
- Industry (manufacturing, service sector, R&D, trade),
- Governance (policy, procedure, statistics, survey, records, administration).

Inter-state political and ideological differences, competition for resources including ‘knowledge’ itself, business rivalries and even terrorism are key drivers and a burden for cyber security in civil domain. Accordingly, civil functions of cyber security aim at securing the cyber-space in a manner as to prevent inimical acts of the following kinds: -

- Sabotage of ‘National Information Infrastructure’ (NII) through intrusion into electro-magnetic spectrum,
- Inducing collapse, corruption or diversion of the nation’s Information Technology (IT) driven public service, administrative, economic, technical and industrial infrastructure.
- Psychological subversion of the society to manipulate public opinion.

The civil functions of cyber security in our context would involve the following mechanisms:-

- Warning and response to cyber-attacks,
- Retrieval of cyber-assets – primary, secondary and tertiary data, protocols and processes, and,
- Restoration of the compromised cyber driven systems – economic, industrial, technological, societal systems.

Cyber Warfare in the Military Domain

- In the military domain, operations that are undertaken to gain information superiority fall under the ambit of ‘Information Warfare’ (IW). Within that ambit, offensive and defensive ‘Information Operations’ (IO) are waged by means of weaponised intervention, electronic warfare etc., ‘cyber warfare’ being one such mean that is prosecuted in the cyber-space. Cyber warfare therefore is truly a ‘military operations of war’, to be conducted as an element of offensive and defensive IO, and waged in the same spirit of ultimate measures. It is distinguished by predominance of offensive content and is to be prosecuted through military-dedicated IT-based satellites, data warehouses, maps, communication net-works, GPS, UAV, AWACs, PGM etc. However, while civil functions are to be operational at all times, the military function during peace-time is to prepare and test continuously, letting go at war-time to disable the opponent’s military, quasi-military and civil infrastructure. Herein lies the distinction between the civil and military functions of cyber security. Conversely, there are many commonalities between the two functions with respect to the above discussed civil cyber security mechanisms as well as the software skills, hardware and processes.[7]

5. NEIGHBOURING COUNTRIES CYBER WAR ON INDIA

Cyber warfare has been an issue for India for a long time now. In the recent years direct attacks has given way to cyber-attacks causing greater damage to India. This is complemented by adequate cyber security and lack of adequate infrastructure thus exposing India to a greater danger. Currently we do not have a cyber warfare policy and no concrete implementable cyber crisis management plan that can be deployed at the time of a cyber war.[8]

In August 2010, the Indian government initiated the steps to strengthen the cyber security infrastructure in India. The strategy was directed to develop capabilities to snoop into network unfriendly countries, setup ethical hacking laboratories, state of the art testing facilities, develop counter measures for possible attacks and set up CERTs for several sectors. The strategy was a joint initiative National Technical Research Organization, the Defense Intelligence Agency, and the Defense Research and Development Organization. During this period, India discovered a Chinese variant of Stuxnet worm in Indian Installations. In addition to the Chinese worm, in December 2010, India’s most secure website of India’s Central Bureau of Investigation was defaced by Pakistan Cyber Army. This reinforced the need for a strong offensive and counter offensive capabilities and laws in cyber security. The second cyber warfare conference, was held in November, 2011 which provided different aspects and case studies to showcase the current scenario and steps to increase the cyber security capabilities.

In October 2012, a government- private sector plan was setup under the guidance of Mr. Shivshankar Menon, National Security Advisor to Prime Minister Manmohan Singh. The purpose of the sector was beef up India’s cyber security capabilities based on the recent attacks. Ironically, India faces a shortage of around 4.7 lakh experts in cyber security despite the country’s reputation of being an IT and software powerhouse.

The new generation proxy war of Cyber warfare, can not only disrupt data-links, electronic devices and networks, but can also use to create panic at a greater extent. Platforms like social media can be used to reach out to maximum number of people in a fraction of second and spread mis-information. We have witnessed the panic caused by Social media in the mass exodus of people of North-East from Bengaluru, Hyderabad and Pune recently. The Pakistan Military Establishment, including ISI, is becoming impatient because of it's inability to create problems in Kashmir region and the lowering of intensity of insurgencies in the North-East.

In the past 65 years after independence, the Pakistan has lost major wars with India. Pakistan has realized that it can never defeat India in a direct war. The Pakistan Militia along with ISI started a proxy war in India consisting of trained Jihadi groups, whose purpose is to create havoc in India through various means. They were successful in creating some noise initially, but their recent efforts to spread terror has been foiled by the Indian Intelligence. Since the terror attacks are failing, Pakistan has started to use their jihadi groups to spread panic using Internet and social media. First, their websites pulled out photographs of violence and disasters from different countries, morphed and uploaded to show violence against Muslims in Myanmar and Assam. Second, they used SMS messages through their sleeper cells in India to circulate threat to all the North-East people working in major cities like Bengaluru, Hyderabad, Pune Delhi etc. The result was that there was mass exodus from these cities due to the threat posed in these messages.

Pakistan successfully used the next generation warfare, i.e. 'Cyber War' and managed to create a false perception of insecurity amongst the people from the northeast. The Indian intelligence agencies were clueless about it and the havoc was created by Pakistan using Cyber cells. The result was almost half a million people in panic left for their hometown in Assam. Although the Indian government raised protest with Pakistan, Pakistan denied all the allegations and asked for proof of the investigation.

The extent to which Cyber warfare can harm a country is unimaginable. Cyber warfare is not limited only to creating Havoc and spreading false information on Social media. At times of War, the adversary can easily manipulate the data, perception and decisions of the opponents. Aircrafts can be neutralized, Missiles can be caused to misfire to create destructions within. The country's transportation, banking system can be neutralized creating a havoc among the people.[9]

Fake orders can be passed to military units including nuclear strategic command. Television transponders can be hacked and forced to showcase fake news, creating further havoc in the country. Jamming of telephone lines, banks and financial institution will bring any country to the verge of bankruptcy. The only successful defense in case of a cyber warfare is powerful offence. The answer to defend our nation against cyber-attack does not lie in regulating Internet or banning social media as demanded by some. There is a need for strong Government policy to strengthen the country's defense against cyber war. India should setup a strong team of cyber Army to defend networks, data links and electronic devices and at the same time launch counter attack on the enemy. India is on the way of becoming the silicon valley of the world and boasts a strong technically skills workforce who can be trained and utilized for this task. [10]

6. THREATS:

Cyber threats can originate from foreign hostile nations or domestic sources like self-proclaimed religious group. These sources could be state intelligence agencies, economic and technological competitors, and foreign military establishments as part of their war preparedness, and lastly, rogue non-state elements perpetrating acts of cyber-terrorism. The threats are characterized as follows:-

- Paralysis of cyber intensive networked systems at the national level to freeze the adversary's ability to function unencumbered.
- The attacker may not easily identifiable, since the attack can be routed through various sources, Even if identified, the system architecture may be difficult to decipher, thus hampering effective counter measures.
- Once the attack is triggered, the cyber terrorist will not be able to control the degree of paralyzing effect that attack can cause. Neither it is possible to contain the damage from affecting unintended parties. The collateral damage in cyber-attack is much more than in terrorism.
- Social media platforms provide easy access for saboteurs to spread mis-information to more number of people at a very less time. Dependence of global cyber assets like internet GPS, digital information has it's own advantage and disadvantages too.[11]

7. CHALLENGES FOR INDIA:

Cyber warfare in India has always been confused with website hacks, email hacking which can be considered as minor cyber security breaches. India has been very late in recognizing a need of the robust cyber security laws and policies. India did come up with the national cyber security policy of India 2013 (NCSP 2013) was declared belatedly and it is still waiting for its implementation. India has no cyber warfare policy till date.

The Indian government should study the various laws and policies in different countries in the West and try to implement the cyber security policies before it's too late. International legal issues of cyber-attacks, cyber terrorism, cyber espionage, cyber warfare and cyber crimes in general and international legal issues of cyber-attacks should be understood by the Indian Government and implemented in Indian perspective. [12]

The Department of Information Technology created the Indian Computer Emergency Response Team (CERT-In) in 2004 to thwart cyber-attacks in India. In 2004, there were 23 reported cyber security breaches, by 2011 it rose to 13,301. In 2011, the Government created a new sub division the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart attacks against energy, transport, banking, telecom, defence, space and other sensitive areas. However, there is no public face of NCIPC and some experts believe that NCIPC has failed to materialise and perform its job. It was also reported that National Technical Research Organisation (NTRO) would protect the critical ICT infrastructures of India.

In February 2013, the Executive Director of the Nuclear Power Corporation of India (NPCIL) gave a statement that NPCIL alone has blocked up to 10 targeted attacks a day. These attacks were on critical sectors. CERT-In was left to protect less critical sectors.

The last known high profile cyber-attack was on 12 July 2012 in which the e-mail accounts of about 12,000 people were breached including some high profile officials from Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organisation (DRDO), and the Indo-Tibetan Border Police (ITBP).

In February 2013, Information Technology Secretary J. Satyanarayana stated that the NCIIPC was finalizing policies related to national cyber security that would focus on domestic security solutions, reducing exposure through foreign technology. Other steps include settings up of cyber cells and isolation of various security agencies to ensure that a synchronized attack could not succeed on all fronts. As of this month, there has not been any significant development in setting up necessary infrastructure to fight cyber terrorism. Fortunately, there had been no significant economic or physical damage to India related to cyber-attacks.[13]

8. CONCLUSION

At present time in India, the development of cyber-assets depend upon how strong protection measure we have devised to protect it. It is the stage when cyber security should be placed at the zenith of priority even if it amounts to certain modifications and alterations in India's cyber domain. If the cyber security of the country is to be preserved the most pertinent consideration is that the security measures must be devised keeping in mind the native conditions and shall be developed by the Indian minds. This consideration again remind us the reason behind formal division of roles and responsibilities between the civil and military functions of cyber security.

Seeking example from 26/11 terror attacks on India's commercial capital of Mumbai in 2008, where the terrorists used computers and satellite phones for having instructions from the conspirators in Pakistan, the Government is ushering considerably towards ensuring cyber security. India has a strong hacking network. Other than this, several operational steps have been announced by the government, such as founding a National Defense University with a key focus on computer software, and establishing a new intelligence communication and electronic surveillance agency. India actively seeks military-technical and scientific cooperation and exchange with strategic partners such as Israel and Russia that reputedly possess exceptional cyber capabilities.

However continuous worms and viruses attacks are to be tackled periodically.

As it is quoted by National Security Advisor Mr. S.S. Menon India needs to "harden its critical networks and develop metrics to certify and assure that our critical cyber networks, equipment and infrastructure are secure" and that "we must find ways to indigenously generate manpower, technologies and equipment that we require for our cyber security."[14]

India needs to prepare ground to tackle with the threats to cyber space and risks arising through cyber space, as a "step towards a coherent and comprehensive cyber security policy. Cyber space is developed as the platform of global governance and the problem of cyber security cannot be tackled by governments alone. Public Private Partnership (PPP) is required.

Even the prime Minister of India now acknowledged that India must be prepared to meet the challenges arising out of Internet and cyberspace.

Another aspect is that when it comes to typical military engagement of cyber warfare, it's still not tested one before a full-fledged warfare so new research and advancement in technology have to be updated and systems upgraded continuously since the enemy cyber warfare preparedness is like a black box. First attack is the final attack. All that is tested full-fledged by hostile states is on civilian space not on military space due to various tactical reasons.[15]

REFERENCES:

1. Lt.Gen.AKS Chandele,(Jan-Feb'2013) Modernisation of the army is a continuous process, Geointelligence, Editorial, Vol.3, Issue 1,

2. Lt.Gen.Gautam Banerjee, (7'Feb, 2014) 'Dimensions of Cyber security in India', Vivekanand International Foundation,.
3. Asif Ahmed, (Feb'16, 2014) 'Cyber warfare and information security for India', Eurasia review,
4. *ibid.*
5. Lt.Gen. Gautam Banerjee, (April'28, 2014) 'Cyber warfare in Indian context', Vivekanand International Foundation, *ibid.*
6. Lt.Gen.Gautam Banerjee, No.2.
7. MasoodUr.Rehman, (June 08'2012) 'Network Centric Warfare Capabilities in the Indian Military', South Asia Strategic Stability Institute, Weekly Pulse, , Islamabad.
8. Staying safe in the Cyber world, Mass.gov blog, 24 Oct 2013, http://blog.mass.gov/blog/safety/staying-safe-in-the-cyber-world/
9. Asif Ahmed, No.2.
10. Lt.Gen.Gautam Banerjee, No.5.
11. NavneetBhushan, (April 28'2012) 'Network Centric Warfare – A Revolution in Search of Indian Doctrine', Frontier India,.
12. Available online, https://en.wikipedia.org/wiki/Cyberwarfare
13. India's cyber security challenges, Institute of Defence Studies and Analyses Report, May 16'2012.
14. Dorothy E.Denning, (1999) Information Warfare & Security, Addison Wesley Longmen, Singapore Pte. Ltd..