JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber Age : India's Future Warfare Strategy

Dhiraj Yadav

Abstract:

Information is the key to sustain in the cyber world. India as part of major emerging and can increase it's domination only by enriching its data understanding and implementation and execution over the impact of data output. For this India has to create its 'National Cyber strategy' and there should be an environment to secure information. It's a need of time to create a 'Cyber Army' in India. India should focus on research and education. There is a need for public-private partnership and people should be aware about cyberspace and its activities.

Keywords: Cyber security, cyber warfare, Cyberspace, Cyber strategy.

"In the cyber world, privacy of information is power"

Information is a basic need for human beings to survive. We are in the 21st century, in the age of I.C.T, that is, Information, Communication and Technology. today there is a huge flow of information all over the world. people are communicating beyond the national boundaries. technology is playing a pivotal role in connecting people to each other worldly. information is the new power in the world system and it is the significant aspect of diplomacy and armed conflict between Nation-states.
As far as International relations as a specific discipline is concerned, technology has been a new foundation of relations between States for years. even citizens at their level sharing and connecting with each other. They share their cultures and ethnicities.

Historical Importance :

From World War 1 and World War 2, technology changed the nature of the relations between Nation-States. Even wars and conflicts have been changed through technology.
In world war 1, warships played a disastrous role and many other battleships and war tanks were invented and took place in wars.
And in World War 2, nuclear weapons were used. In 1945 America bombed nuclear weapons over Hiroshima and Nagasaki. these and atomic bombs changed the nature and impact of War.
The two atomic bombs dropped on Japan in 1945 killed and maimed hundreds of thousands of people and their effects are still being felt today.
By the end of 1945, the bombing had killed and estimated 140,000 people in Hiroshima and a further 74,000 in Nagasaki in the years that followed many of the survivors would face leukemia,cancer or other terrible side effect from the radiation.
The uranium bomb detonated over Hiroshima on 6th August 1945 had an explosive yield equal to 15,000 tonnes of TNT. It razed and burnt around 70 percent of all buildings and caused an estimated 140,000 deaths by the end of 1945, along with increased rates of cancer and chronic diseases among the survivors. There were long term side effects that it takes around 10 seconds for a fireball from a nuclear explosion to reach its maximum size but the effects last and span across generations.
Five to six years after the bombings the incidence of leukaemia increased noticeably among survivors. After about a decade, survivors began to have other cancers at higher than normalrates.
Pregnant women exposed to the bombing experienced higher rates of miscarriage and death among their infants. their children were more likely to have intellectual disabilities impaired growth and an increased risk of developing cancer. and for all survivors, cancer related to radiation exposure still continues to increase throughout their lifespan even to this day seven decades later. So this is how Technology affected the nature of the conflicts and wars in this world system. After World War 2, Many other modern weapons were invented like modern tanks, missiles, Cruise missiles, ballistic missiles, BMD (ballistic missile defence) systems and drones etc. They had changed the type of wars and they affected the nature of War. But after the invention of INTERNET, human life changed a lot. today a person can't live without a scrolling screen.

People are very busy on social media. they post their life events, pictures and photos and they share their ideas. they comment on all type of issues, prevailing in society. People are getting and sharing more information and they put their identities in public on social media. So this excess of information changed the patterns of privacy. Thus security took place here in this world of information. Security of information is necessary.

Contemporary Dynamics :

Cyber crimes are increasing a lot. hacker's groups, other foreign state or non-state actors like terrorist groups try to unlock the security of people's information on social media. They try to hack the computers of the government. They want to get internal information from government agencies and institutions. They use that information for their benefits, they demand money or crypto currency in the exchange of your information.

So this should be considered as a server crime and when a state uses cyber attacks in a particular cyberspace against it enemy state or an enemy State uses against a state. It is called cyber warfare. Its impact is comparable to actual Warfare. This Warfare disrupted all the computer systems in a particular department or any digital infrastructure of any agency or institution. Many times these attacks result in espionage, sabotage, propaganda, manipulation or maybe economic warfare. In that situation a country should take particular measures to protect information. If we talk about India, it should take a stand to protect information according to a particular strategy.
Indians should create a culture or environment to understand the seriousness of these types of attacks. People of India should be aware of the privacy of their information. At the military level India should create a cyber army or body to protect the information of Indian people and Indiangovernment.
Countries like the U.S.A, Russia, China, Israel, Iran and North Korea dominate this domain. They use both offensive and defensive strategies in cyberspace.
India is observing the situation of the present time and taking steps for the future. it is doing its best, going towards cyberspace. India is implementing e-governance, e-economy, online AADHAR and many other programs regarding education, medical etc.

Understanding Cyber Dynamics :

- Cyberspace

Cyberspace is a platform or area where there is a network of information and data and the
network of computers. It consists of the activities like sharing of data, hacking and protection of data and information, which occur in an environment of information. the internet is considered as a cyberspace but it is not so. The Internet may be the first and foremost or basic component of cyberspace.The Internet was originally conceived of and funded by American Defence Department's research organisations, then known as the Advanced Research Projects Agency (ARPA). Given the state of telecommunications and the non-networked computer systems that existed in the 1960s, researchers wanted to create a reliable network where a user's system or location was unimportant to his or her ability to participate on the network.
This vision of a network became a reality in 1969 when a computer link was established between the University of California-Los Angeles, the University of California-Santa Barbara, Stanford University, and the University of Utah. At the time, the connection was called "internet-working," which was shortened to Internet. For thirty years, the Internet was largely the domain of universities, colleges, and research institutes. But when Tim Berners-Lee and his colleagues created the World Wide Web (WWW) in 1990, commercial and social applications exploded.
Within a few short years, companies like Amazon.com and eBay (1995), Wikipedia(2001), Facebook (2004), Twitter (2006), and Snapchat (2011) founded a new industry and changed theway we live and work.
The development of the information environment has been influenced by science fiction, which offers both inspiration and anxiety for thinking about technological change. Writer William Gibson coined the term "cyberspace" in a short story published in 1982. Once confined to the cyberpunk literature and science fiction like the movie The Matrix (1999), the information
environment entered the real world in the late 1990s, and in 2003 the Bush administration defined cyberspace as the "nervous system-the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre opticcables that allow our critical infrastructures to work." The U.S. Defence Department later defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications network, computer systems, and embedded processors and controllers." When we add people and the decisions they make to the cyberspace definition, we have the information environment.
According to Myriam Dunn cavelty,Cyber space connotes the fusion of all communications networks, databases, and sources of information into a vast, tangled and diverse blanket ofelectronic interchange.
A Network ecosystem is created it is virtual and it exists everywhere there are telephone wires, coaxial cables, fibre optics times or electromagnetic waves (Dyson et al. 1996) however cyberspace is not only virtual, since it is also made up of servers, cables, computers, satellite, etc. Cyberspace and 'Internet' are used almost interchangeably but the Internet is just one part of cyberspace.
According to Christopher and Brian,
In their book titled Understanding Cyber Warfare Politics, Policy and Strategy, Christopher Whyte and Brian Mazanec give the definition of cyberspace as a fact of daily life in the twenty-first century. It is the unusual political episode or diplomatic incident that occurs without feeling the modifying influence of the digital world. Cyberspace affects the real-kinetic dynamics

of everyday global society at almost every level-virtual networks aid in the spread of information about a particular issue, while different computer systems serve as a direct path between the functions of different national or subnational institutions and, in doing so, has a very real impact on policy, politics, and security.

- Cyber security

To understand the term cyber security, firstly one should understand the term security which consists of two aspects. First one is 'protection' and the second one is the 'absence of insecurity'. So cyber security confers the insecurity created by and the practices and process to make secure the information in a cyberspace. Insecurity, that is, attacks or threatening of objectives or values of state and society, cyber security confers as a sphere of operations and measures to protect information and data.And now further there are few "cyber" terms (i.e."cyberwar," "cyberterrorism," "cyberbullying," "cyberspace," etc.) for which there is universal agreement on what is exactly meant. Cyberspace is a particularly slippery concept. Cyber- security, likewise, would be tricky to define if you were to ask a diverse enough audience. From a purely technological perspective, cyber-security is constituted of all processes, procedures, design considerations, and actions concerned with the security of information systems. This means that anything bound up in protecting computer systems and the networks that connect computers from attack, disruption, and infiltration constitutes cyber-security. In reality, this definition is, roughly speaking, one likely to receive broad approval by practitioners and scholars across the fields concerned with cyber-security.

Insecurity agents

In cyberspace attackers or criminals who infringe the privacy or get the information or disrupt the information infrastructure, are called Hackers. They are very skilled programmer, technical experts. They can be traced as social groups or they can be foreign States. They may be criminal groups or hackers, hactivists etc. they can be disgruntled insider or they can be terrorist too.

All these agents use the information for their personal interests.

- Hacking tools

Hacking is seen as 'modus operandi' that can be used not only by skilled technical individuals but by foreign states or terrorists too. They use some tools to infringe the privacy of one'information and these tools become the causes for attacks on a State as cyber insecurity.

Virus: Malicious code that can self-replicate and cause damage to the systems it infects. The code can delete information, infect programs, change the directory structure to run undesirable programs, and infect the vital part of the operating system that ties together how files are stored. Worm: Similar to a virus, a worm is distinctive for its ability to self-replicate without infecting otherfiles in order to reproduce.

Trojan horse: A stealthy code that executes under the guise of a useful program but performs malicious acts such as the destruction of files, the transmission of private data, and the opening of a back door to allow third-party control of a machine.

Logic bomb: Camouflaged segments of programs that destroy data when certain conditions aremet.

Zombie: A computer that has been covertly compromised and is controlled by a third party. Botnet: A network of zombie machines used by hackers for massive coordinated system attacks. Denial-of-service: Attack employing a botnet to send massive simultaneous requests to servers, preventing legitimate use of the servers.

Defining Cyber warfare :

Cyber warfare is a type of continuous conflict in cyberspace. In this type of War enemy state or any hacker group or terrorist groups attacks on computers through any spyware or any malicious software to get the personal information or data. countries are going towards e-governance and e-economy because of technical development and development of the internet. work is being done on computers. National structures like oil infrastructure, military infrastructure, nuclear plant or Railways or electricity plant etc. are working online and all the data and information are saved on computers. Due to this online information, Cyber Warfare took place, so, it's necessary need to save the information from hackers or foreign state or terrorist groups.

As far as India is concerned, in India things are changing a lot. India is going towards e- governance and e-Commerce rapidly. all the information is on governmental sites. Internet users are also increasing in India; they are 47% of its population. so, people are also using online platforms like social media platforms. Nowadays, problems like fake news, rumours on social media causes for communal disharmony or cyberbullying, cyber manipulating, are increasing.

On the other hand states like China and Pakistan are attacking India's information infrastructure. So India should take specific measures to deal with problems and we will further discuss some steps to take to deal with and to save the data and information.

At the world level we can observe that countries like the USA, Russia, North Korea and China etc are fighting cyber wars and recently a war between Russia and Ukraine took place. It is not only a physical war but also a cyber war. Russian cyber agencies became active and attacked the Ukrainian information infrastructure. Some other hacker groups like ANONYMOUS etc. are also playing an active role in the war. It is also attacking Russian information infrastructure.

So it can be said that cyber warfare is the war for information.

Here are some case studies which define cyber warfare.Case studies:

1). Pegasus controversy in India. Pegasus is malicious software and it is designed to gain access to devices without the knowledge of users. It has been developed by the Israeli firm NSO group. In India it is reported that this spyware was used

on ministers, opposition leaders, political strategists and tacticians, journalists activists, minority leaders, administrators like election commissioner and head of central bureau of investigation. According to the report covered by New York Times, it was said that the Indian government has purchased Israeli NSO group's Pegasus software in July to 2017 in order to carry out targeted surveillance on citizens, climbing that high level visits by P.M. Narendra Modi and former Israel Prime Minister Benjamin Netanyahuand even a U.N. vote on a Palestine Organisation was part of a large backroom deal.
In the report published on January 28 The New York Times said that ties between PM Modi and
P.M. Netanyahu had 'warmed' because of their agreement for the sale of a package of sophisticated weapons and intelligence gear worth roughly $ 2 billion with Pegasus and a Missilesystem.
Because of this report published in New York Times, the opposition parties attacked the government accusing it of misleading Parliament and the Supreme Court on the issue. While, Congress party said the alleged use of spyware on opposition leaders, Supreme Court judges,journalists and activists, was an 'act of treason'.
But the Modi government denied all the blames claimed by the opposition. The Supreme Court established a technical committee to examine this case.

- India-china cyber warfare

China is running a cyber espionage campaign. it is expanding cyber threat against India

There is a huge tussle between India and China. China attacked India's information infrastructure many times. there are many examples of attacks done by China on India such as-
on 6 April 2022 American cyber security firm, RECORDED FUTURE revealed that Chinese state sponsored hackers had targeted India's Power Grid in Ladakh.
In March 2021 Singapore based company Cufrima revealed that a Chinese state backed hackers group had targeted the Information Technology system of two Indian vaccine makers– Bharat Biotech and The Serum Institute of India. Maharashtra government's technical audit committee reported that 'RedEcho' a China - linked hacker group had breached the Indian power sector which may have caused Mumbai's power outage. Chinese hackers also targeted two Indian ports and some parts of railway infrastructure. China attacks on information infrastructure for getting commercial benefit or for creating products according to consumers in foreign countries and China also attacks for technical benefits like attack on defence technology of enemy states.
India also has a comparative advantage which includes India's startup innovation ecosystem with which India has barred Chinese investment.
But to deal with Chinese cyber espionage attacks, India should extend its offensive and defensive measures. There is need to do more.
On the other hand, Pakistan is becoming the proxy of China against India. China and Pakistan have their long term benefit plans collaboration like 'China Pakistan economic corridor 2017 2030.' Pakistan, in the influence of China, is creating anti-India propaganda on social media. There is a need for India to fight China–Pakistan cyber warfare well.

Indian Cyber Dynamics :

People of India are very busy on social platforms. Social media has emerged as a separate type of mass media and it has a direct impact on society and democratic structure of the country. So it is very essential for India to protect the information of its agencies and institutions. And if India wants to take this cyber power. it should create an environment to protect the information from cyber attackers and hackers. it should adopt both offensive and defensive studies in this cyber warfare. India should create a body of cyber army. People of India should be awakened for their privacy of information. they should know the uses and misuses of social media. they should be aware of Cyber hacktivism and cyber manipulation etc. But in actuality, situations and conditions are different. According to the department of telecommunications, in India, internet users are almost 47 percent of its population. So this creates a huge digital divide. Many of them are not aware of cyber espionage, cyber hacking and manipulation etc.or even about the internet.
This creates some basic questions like 'Is India facing the problem of cyber warfare and cyber insecurity?' 'What is the meaning of cyber warfare in the Indian context?' 'What should be the strategy and what should be steps to create an environment and culture to protect the information, if there is a problem of cyber attacks in India?' 'How will India create awarenessamong Indians for the privacy of information?'

Gateway for India’s Cyber Future:

- National cyber strategy

India should form its strategy according to its experiences. India should observe its internal events which occur in its domain of Cyberspace. attacks which have been done in India, hacking in Indian Institutions, India should analyse all the things and it should analyse the types of information, its importance according to its use and benefits. India should know the level of Indianpeople in the world of Cyberspace how are people dealing with this cyber insecurity?
India should analyse the impact of cyber attacks and those laws which are available earlier. it should know that these pre-existed laws worked in reality or not. If yes then India should amend these laws and bring new ones.India should know the scope of strategy and what it consists of. Security refers to the mechanism of development and it confers national power as its own instrument. strategy should be form according to its objectives and aims.India is a rapidly emerging power. it is putting its steps towards E-Governance, E-Commerce etc. In India, institutions like Railways, nuclear plants, Space Agency ISRO, power grades, oil infrastructure etc. all these institutions have their online infrastructure. They are working online and storing their information on computers.
People of India are becoming aware about online information. They are using social mediaplatforms.
By observing the situation, Indian government has brought some programs and initiatives -

- Cyber Surakshit Bharat
- Cyber Swachhta Kendra
- Online Cyber Crime Reporting Portal.
- Indian cyber crime coordination centre (14c).
- National Critical Information Infrastructure Protection Centre(NCIIPC)Information Technology act, 2000. National Cyber Policy 2013 etc.

- India has its agency called Defence Cyber Agency, for its armed forces which deals with the attacks done by enemy states.

India is the second fastest digital adapter among 17 of the most digital economies but there is a strict need to increase its information infrastructure in the fields of e-commerce and e- governance. India should have its own social media platform like Facebook, WhatsApp or twitteretc. It is because, many times
we hear about the leakage of information on these foreign private social media applications.

- National cyber security policy

Decision-making or formation of policy is being done according to conditions and experiences, which are prevailing in the society. India has taken some initiatives which have been mentioned earlier like Cyber Durakshit Bharat initiative, Cyber Swachhata Kendra, Online Cyber Reporting Portal and Information Technology act 2000 etc. But these are not enough. India should be more visionary. It should focus on the future significance of cyberspace. It should know how cyber warfare is emerging as a new warfare as a warfare of information.
So, India should set it's locus of security towards the problems of future and to deal with these types of problems like loss of privacy, cyber hacking, cyber bulling or loss of private of Information and cyber terrorism etc. India should take some basic measures which are following-:

- An environment to secure information

There should be an environment to understand the functioning and the problems of Cyberspace.
There should be awareness and understanding among people to use
cyberspace, social media and online apps or e-market safely. The government should create a culture to protect information in every institution so that data and information could be protected.

- Cyber Discipline

There should be a cyber discipline in the country. In cyberspace, every institution or agency of government should follow particular rules and regulations so that information can be protected. people should not face cyber manipulating, cyber terrorism or hacktivism and infringement ofprivacy.

- A cyber security organisation

Every department of government should have a cyber security organisation, so that this organisation can work for protecting information.
At the centre there should be a 'guidance organisation' that can guide the organisation in adepartment.
There should be a 'co-ordinator' or a 'technical head' in every department.

- Cyber research and education

The Indian government should propagate Research and Education in the field of Cyberspace. There should be particular rules for 'Primary' 'Secondary' And 'Higher' cyber education.
There should be separate disciplines and courses for Cyber research. students should learn ethical hacking. they should learn to protect data and information. So, India should focus on the specific study of cyber research and cyber crimes so that people should be aware of and an environment of protection of information and data can be created

- Cyber security army- militarisation

There should be recruitment for Cyber Army or we can say that militarisation should be done in cyberspace. there should be a 'body of Army' which can deal with foreign cyber attacks, cyberterrorist and hactivists.
In India, in all the three forces, there should be a wing of :cyber security force' which should work on protecting the information only.

- Civilian and army - work together

Civilians and the army should work together to deal with cyber warfare.
In situations of loss of information, army and civilians should work together. Civilians should be awakened. They should know some basic things like hacking tools,softwares or spywares and cyber crimes etc. they should use social media smartly. So, through the combined work of peopleand army, India would be the power of cyberspace.

- Strict policies and laws

India should formulate some strict policies and laws to deal with cyber crimes. It is because Cyber crimes also have impacts as other crimes. these crimes maybe cause of loss of life, communal disharmony in society or maybe a terrorist attack etc.

- Public-private partnership

It is a big challenge for Indian cyberspace that the private sector is not participating and working with the public sector. if there should be a public private partnership, the efficiency would increase. we can protect our data and information more. In every private organization there should be a cyber authority which can deal with cyber attacks and particularly in an e-

commercial agency for protecting information and these agencies should work with the government.

- Defensive and offensive strategy

Like the USA, India should also adopt both offensive and defensive strategies. If India would like to save its information from enemies. it should also know every information of the enemy. the enemy is attacking us,we should also take offensive measures and should attack on enemies to know private information of the enemy country.By creating a cyber army and skilled persons, Indiacan implement its both offensive and defensive model of strategy.
As Sun Tzu said in his book 'The Art of War' that "attack is the secret of defence and defence is the planning of an attack. Derek S. Reveron also emphasised in his book 'Human and National Security understanding transnational challenges',cyber as a large piece of national power that includes diplomacy, foreign assistance, sanctions and conversation and military power. Bearing this in mind, the Indian Government's strategy should be created as both offensive and defensive.

- Awareness

It's a basic tool to get power in the cyber world or any type of power. Awareness of people is very necessary. India should initiate such programs through which people can be aware about cyber attack, cyber crime and tools of hacking or cyber espionage etc. many times we see that people face cyber fraud and they even don't know what happened with them. Generally people face money fraud on many online platforms and sometimes people order anything online but they are cheated. So, people should be aware of e-market cyber crimes. many children face the problems of extortion, sometimes it causes for suicide too.
By bearing all these issues in attendance, India should initiate programs and issues and some guidelines, through which people should understand the importance of privacy of information. they should not share any important information to someone anonymous or authority or online agency, which can use it for their benefit. People should be aware all the time while clicking anylink or downloading any app or giving access to private information to any app or any site.
On people's side, they should also be authentic on social media. They should be responsible for their comments or posts or on social media platforms.
So, people should understand these things and play an important role in building power for thenation.

Conclusion :

Cyber warfare is continuous warfare. There are no time conditions in this Warfare. Any attacker or hacker can attack any time. India should prepare all time with its strategies. India should have a National Security Strategy with specific policies and laws. To deal with countries like China, India should adopt offensive and defensive strategies. It should spend more money on cyber Research and technical development. Though India has its big information infrastructure in many institutions like railway, oil or food infrastructure, army weapons institution etc. It has laws and acts like IT act 2000 etc. For the first time, during the government of Rajeev Gandhi, technological and computer infrastructure was introduced in government offices.
But bearing the present experiences and future ideas, India has some basic needs to reform its education system. there should be reforms at the societal level. People should be more aware and knowledgeable to deal with cyber in-security because cyber warfare is psychological warfare.
India should be prepared psychologically by focusing on future cyber infrastructure.

Resources:

1- https://www.icanw.org/hiroshima_and_nagasaki_b ombings/
2- Reveron,Derek S. Human And National Security Understanding Transnational Challenges. New York: Routledge, 2019.
3- Collins, Alan. Contemporary Security Studies (Article-: Cyber security by Myriam Dunn Cavelty). Oxford: Oxford University Press, 2019.
4- Whyte, Christopher, Brian Mazanec. Understanding Cyber Warfare Politics, Policy and Strategy. New York: Routledge, 2019.
5- Whyte, Christopher, Brian Mazanec. Understanding Cyber Warfare Politics, Policy and Strategy. New York: Routledge, 2019.
6- Reveron,Derek S. Human And National Security Understanding Transnational Challenges. New York: Routledge, 2019.
7- https://www.thehindu.com/news/national/pegasus- and-a-missile-system-were-centerpieces- of-2-billion- deal-between-india-and-israel-in-2017-nyt/article383 43251.ece
8- Collins, Alan. Contemporary Security Studies (Article-: Cyber security by Myriam Dunn Cavelty). Oxford: Oxford University Press, 2019.
9- Whyte, Christopher, Brian Mazanec. Understanding Cyber Warfare Politics, Policy and Strategy. New York: Routledge, 2019.
10- https://www.orfonline.org/expert-speak/expanding-ch inese-cyber-espionage-threat-against- india/