WAR WITH NO HUMAN

Rahul Gaur[1]

ABSTRACT

Cyberwarfare though sounds like war but is the new and latest trend of war. It is conducted on computers by humans in virtual form and most important of which there is no loss of human life but still the other nation is defeated. There exist various countries like the USA, Russia, China who have become a super power in cyber warfare but countries like India are not only lacking but they are still waiting for something big to happen to act on it. This paper tries to convey a basic idea to its reader about cyberwar and how it has transformed from a theoretical concept to a practical approach. Also, the lacking of any framework both at the national and international level is shown and the current position of India is also highlighted and also various steps are suggested as to how to combat this latest trend and most dangerous form of war. Also as it is not only the latest but also it is impossible to identify that either a country was attacked with it or not and even if after identification it is impossible to stop it and find anyone guilty as there is no proper framework for the same. So we can say that it is a war with no limitation and no norms and most cruel of any form of war.

INTRODUCTION

Cyber Warfare is only a battle with the assistance of PCs to upset the ongoing functions of the state to make hurt the other country. It equivalent to customary war however it is on PCs and battle without people, in short, we can say it as battle without any people. Though cyberwar being a new concept, it is used mostly because of its techniques and way of conducting the same. Though there exist various laws to regulate the same both at the international and national level but they have to experience the most common drawback that is the implementation of the same. This form of war earlier exists only in theory but with the help of the latest examples, we can consider it as a practical and most dangerous aspect of any war for which only a few countries lead the same and others are pourable in front of them and they even can't protect themselves as UN also has not passed any resolution for the same even UNSC has also not coined the same issue because this power is handled by them only

[1] B.B.A LLB, FOURTH YEAR, NEW LAW COLLEGE, B.V.P.U, PUNE.

and to maintain their dominance they want to let this issue to addressed unless and until a major war will launch with this method. Further various aspects of cyberwar and its legal aspect are covered and in end, there are various suggestions are given to deal with such a war from the Indian point of view.

DEFINING CYBER WARFARE

"Cyberwarfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, intending to create damage, death, and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles." "Sending soldiers into trenches and onto the frontline is no longer necessary as the hell of war is increasingly conducted online. This is called cyber warfare and it involves the use of technology to attack other nations, governments, and citizens by attacking their computer systems."

"Cyberwar is usually waged against government and military networks to disrupt, destroy, or deny their use. Cyberwar should not be confused with the terrorist use of cyberspace or with cyberespionage or cybercrime. Even though similar tactics are used in all four types of activities, it is a misinterpretation to define them all as cyberwar. Some states that have engaged in cyberwar may also have engaged in disruptive activities such as cyberespionage, but such activities in themselves do not constitute cyberwar."[2] In simple words, we can say that cyber warfare is the use of hacking techniques by the person authorized by the government of a particular country to take secret information of another country or to cause any form of damage to the attacked nation.

LIST OF LAWS WHICH CAN BE USED FOR CYBER WARFARE

Cyberwarfare can be dealt with the help of the following laws:-

1. Tallinn manual
2. Information technology act 2000
3. Cybersecurity act 2013
4. Space laws
5. The international peace treaty(Vienna Show, extra convention 1, and so on)

[2] John B. Sheldon, Cyberwar, britannica, https://www.britannica.com/topic/cyberwar

6. United nations digital protection measures
7. Cyberspace laws

HOW IS CYBER WARFARE CONDUCTED

"Nation/State-sponsored hackers (hackers either in the military of a nation/state or supported by the said state) attack computers and networks that are involved with sensitive resources within a country. They do this like you would hack any other computer or system: you learn as much as you can about the system, you figure out its flaws, and you exploit those flaws to either gain control of that system or destroy it."

"The cyberspace domain is composed of three layers. The first is the physical layer, including hardware, cables, satellites, and other equipment. Without this physical layer, the other layers cannot function. The second is the syntactic layer, which includes the software providing the operating instructions for the physical equipment. The third is the semantic layer and involves human interaction with the information generated by computers and the way that information is perceived and interpreted by its user. All three layers are vulnerable to attack. Cyberwar attacks can be made against the physical infrastructure of cyberspace by using traditional weapons and combat methods. For example, computers can be physically destroyed, their networks can be interfered with or destroyed, and the human users of this physical infrastructure can be suborned, duped, or killed to gain physical access to a network or computer. Physical attacks usually occur during conventional conflicts, such as in the North Atlantic Treaty Organization's (NATO's) Operation Allied Force against Yugoslavia in 1999 and in the U.S.-led operation against Iraq in 2003, where communication networks, computer facilities, and telecommunications were damaged or destroyed."[3]

"Information on the Internet is exchanged through packets of data sent by computers to each other. A file or request for information is divided up into these packets to make the load manageable for the computer to process and the Internet connection it travels over. Each packet can carry up to 1500 bytes of information. Each byte is comprised of eight bits of data. Each bit can either be a zero or a one. The byte system allows what humans read as words or numbers, as well as logical processes within computer applications, to be transferred from one place to another in binary. Binary is a language entirely comprised of ones and zeros. One represents true and zero represents false. A computer at its base level reads these and

[3] John B. Sheldon, Cyberwar, britannica, https://www.britannica.com/topic/cyberwar

zeros and can execute any function it is told to do. Essentially, binary acts as a set of instructions for the computer to follow."[4] The hackers or so-called cyber soldiers use the advantage of this online stored database as it can be accessed from anywhere in the world and by sitting anywhere they can access it and can also hack and enter in its private zone with the help of coding. What they have to do is to send a request and once they are entered they can do whatever they want and no one can easily catch anyone, if somehow they come to know about the same, first it is impossible to know who that person is, if somehow they come to know, they cannot catch him as he is in other country and might or might not that country will help another country to catch that person as it is sponsored by them only.

FORMS OF CYBER WARFARE

There exist two broad forms of cyber warfare and under it exists various methods to conduct the same. These two forms are:

- **Espionage**

"Espionage is taking information that wasn't meant for you. In the case of cyber warfare, you're going to be stealing tactical and strategic information: information about troop movements, the strengths, and weaknesses of weapon systems, the dispositions of various and anything else about sensitive (read: necessary to wage war) resources that might be important to know."

- **Sabotage**

"Also called "direct action," this is when we take an active role and go out there and do something. In cyber warfare, sabotage can be something as benign as dropping a government's website to causing a nuclear meltdown at a nuclear plant. It's a pretty broad term, however, it means "do something" whereas espionage here means "learn something."[5]

CYBERWAR EXISTS IN REALITY OR JUST IN PAPERS

- **"Kosovo War:** May 7, 1999: During the Kosovo War, a NATO jet bombed the Chinese embassy in Belgrade because it was providing communications support for

[4] Khursheed Ansari, Where are all the data on the Internet stored? , Quora, August 6, https://www.quora.com/Where-are-all-the-data-on-the-Internet-stored

[5] Quora Contributor, How Does Cyber Warfare Work? , forbes, ul 18, 2013,12:45pm EDT, https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#4ee6e7d144ce

the Yugoslav army. Less than 12 hours later, the Chinese Red Hacker Alliance formed up and retaliated by launching thousands of cyber-attacks against U.S. government websites."[6]

- "The government of the eastern European state of Estonia announced plans to move a Soviet war memorial, it found itself under a furious digital bombardment that knocked banks and government services offline (the attack is generally considered to have been Russian hackers; Russian authorities denied any knowledge). However, the DDoS attacks on Estonia did not create physical damage and, while a significant event, was not considered to have risen to the level of actual cyber warfare."[7]
- "On December 2019, Russian government hackers targeted Ukrainian diplomats, government officials, military officers, law enforcement, journalists, and non-governmental organizations in a spear-phishing campaign."[8]
- US government alleged that the Chinese government has stolen its stealth fighter jet technology F-22 and F-35 and with the help of the stolen technology the china is developing its various 5th generation stealth fighters like J20 and various others in the list.

INTERNATIONAL PROCEDURE CONTROLLING FOR CYBER WARFARE

If we see for the international conventions and treaties there exists only one major manual which is formed by the members of the NATO countries? A few of the points covering cyber warfare are:

- The manual accommodates sway, purview, and control of state according to the network safety on its region. Rule 1 accommodates the ward of the state to make any law for its digital protection inside its domain and not meddling in any other nation's network safety. Rule 2 accommodates the locale of the state to practice its control over any individual of the state. What's more, rule 3 of a similar part accommodates control of the state over its domain and manage them with no obstruction.

[6] Jeffrey Carr, Real Cyber Warfare: Carr's Top Five Picks,Forbes, Feb 4, 2011,12:44pm EST, https://www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks/#7bdd8f512ef5

[7] Steve Range, What is cyberwar? Everything you need to know about the frightening future of digital conflict, ZDNET, December 4, 2018 -- 10:19 GMT (15:49 IST), https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

[8] Significant Cyber Incidents, Significant Cyber Incidents, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

- According to rule 18, the United Nations Organization can lead any demonstration to advance network safety with respect to the insurance of ever one. What's more, these demonstrations are not considered however unlawful under the manual as it very well might be accomplished for the government assistance of everybody and in doing so somebody may need to endure things.

- Rule 85 discusses the aggregate punishment for doing such an act and rule 95 discussions about the impartial locales which are neutral for all and nobody has authority over it like Antarctica.

This is the single manual which is to control digital war and it is related with various deals to overseeing its enforceability and not pertinent totally on the states which are not the people from United Nations gathering. The comparable doesn't approve any country to follow it as it simply obliges the standard that how the computerized war or digital assaults are to thwarted and taken care of. Likewise, for its enforceability, the Vienna Convention should be bored to consider someone to be at risk.

LAWS IN INDIA AS TO REGULATE CYBER WARFARE

To direct digital war or cybercrimes in India there are two laws Information Technology Act 2000 and NCS Act 2013.

- The National Cyber Security act 2013 was established around then there was a lack of individual or people managing digital protection as today additionally there are just 550 approx. the individual dealing with entire India's network safety. As to satisfy this lack the public authority has established this go about as to offer significance to ICT and network protection of the country. As they beneficiary 500000 people for India's network protection with 24 hours network safety to the country and to give safe digital economy to the regular citizens and military for doing their capacities viably and productively. This act just discusses how to accomplish network protection however not discusses precisely how to manage digital battle as these individuals are simply designated to give financial and correspondence protection to the individuals yet in the safeguarded area there isn't however much accentuation is given then

it was normal. This arrangement is much the same as a rule on how to safe monitors our economy from others and not on the best way to be protected watchmen us from digital wars.

- Also section 70A of the IT Act, 2000 provides for the formation of the Nodal Agency to keep a check on the acts done by people on the internet, and section 69A provides power to the government to block access to public domains if it involves any form of threat to the citizens of the country. But as such, there exists no specific law or rules or guidelines to either form a defensive measure against the cyberwar if one caused.

India doesn't have adequate measures to shield itself from digital war nor it has suitable work power, if there exist a few arrangements, at that point, it is simply restricted to the domain of India i.e., India is missing appropriate framework and laws to manage cyber wars and attacks appropriately. Furthermore, it is missing particularly to adapt up to different nations.

INDIA'S STAND IN CYBER WARFARE

"Since 2018, the military has been working behind the scenes to set up a force to handle cyber warfare, picked from all corners of the Indian Air Force, the Army and the Navy with expertise in the domain to assist in such operations. The Defence Cyber Agency (DCA), coordinating with the NCS Advisor (NCSA) will work and has reportedly got around 1,000 people working out of the Army, Air Force, and Navy. The DCA will make use of the Indian Army's indigenously-developed Bharat Operating System Solutions (Boss) which will have helped in guarding the Indian Army's communication network to date."

. "With the web client base expanding constantly, and more gadgets associating with the web, the digital danger is basic and India needs to improve its current frameworks to ensure the adversary doesn't penetrate its safeguard easily, Indian specialists stress that China could agitate their PC networks during a conflict. One expert believed that a specific reliance on Chinese gear may give China an "enduring" renouncing of-organization limit, One refined attack on an Indian Navy headquarters used a USB vector to associate the "air-opening" between a compartmentalized, autonomous association and the Internet" The Indian Army still can't seem to create anything distantly looking like the Chinese NEW approach including digital fighting and electronic fighting.

CONCLUSION

There are no different laws for the equivalent and in India, there are no fitting framework and strategies to guarantee its network protection and shield itself from digital war. What's more, because of lack of law the ID of the individual who behaviours war is absurd however it is attempted to distinguish by the scientist by contrasting it and customary war. The current situation of India is likewise indicated which shows that India can't shield itself from digital battle in any circumstance. India needs both public and global control for halting digital wars and the absence of dynamic individuals and independence of the nation to shield itself from a digital assault and war. Furthermore that India is from all the side adjusted with its foes so to be with no dread of being dispatch digital assault by different India needs to safe gatekeeper itself and representative the necessary number of the individual to do as such.

To improve its situation India has to focus on developing new infrastructure to defend itself from cyber war. The Indian armed forces have started a good initiative in this field in 2018 but as is the nature of Indian diplomats and bureaucrats that unless and until something big happens we don't act, same is happening now also we are waiting for someone to attack us so that we can act. India is far behind its major enemies like China and Pakistan as they both have dedicated cyber teams in here army. India has to as soon as possible establish a cyber-team in its armed forces to defend itself from such attacks and also to allot a separate budget and training for such a development. In simple words, we can say that India has a long road ahead to cover, so it has to start as soon as possible and also India has to take initiative to make national laws and use its diplomatic channels at the international level to force the international community to take a view and take preventive action at the international level to stop it.