CYBER WARFARE:

NEED OF THE HOUR

BY-ADITYA KHATTRI

Introduction

Modern society is largely dominated by technologies. We have been able to integrate computers in nearly every field of work. Computers have simplified our work to a great extent but have also left us vulnerable to adversaries that are attached to it. Cyber crimes, fraud and other such activities have become common now. Cyber and technology has also opened gateway to a new kind of battle. This kind of warfare is known as CYBER WARFARE. In this the battlefield is more diverse. The rules of engagement are different and the effect is quick. This new kind of warfare requires less budget than traditional warfare and in this victory is for those who dominate minds of their enemies. For a developing and economic country like India cyber warfare is a need of the hour.

What is cyber warfare?

Let us now understand what cyber warfare really means. It refers to use of computers, internet mainly dark web and other activities like hacking or use of spyware to harm enemy without actually deploying troops and other forces. Now days almost everybody has access internet and most of the people take cyber security very lightly which makes them a potential target for cyber hacking or cyber fraud.

Economic Empact:

For any powerful country its economy is its biggest weapon and economy mainly dominates country’s military power. Owing to this we have to understand that attacking financial infrastructure by hacking is pretty much possible. If it is employed then one nation may be able to cripple economy of any nation by spending very little amount. Stock exchanges, banking infrastructures form the stem of economy and any successful attack on them would mean total collapse of economy and will have devastating consequences. In 2017 many countries including UK and Ukraine were hit by a series of viruses categorized as ransom wares. These viruses blocked CPUs and asked ransom in bit coins to release data of those CPUs otherwise data was either erased or leaked. It had very deep impact on UK’s health department. One of the largest shipping company Mearsk was also hit by this and suffered financially.

Cyber Sabotage:

Another tactics of cyber warfare is sabotage and denial of services. In this infrastructure of national importance and other such projects are breached via hacking in order to render them worthless for use. These include government installations, power grids, online transactions, supply chains, fuel supplies, transportation, and communication. Many reports float on internet regarding such activities. One such example is Stuxnet which is believed to be responsible to delay Iranian nuclear program. Attack on power supplies become very dangerous as they affect variety of activities in that region and binds authorities from taking any kind if actions. Many countries claim that there power supplies were hacked. For example Russia claim that in June 2019 there power supply were attacked by US based hackers. Indian Government also claims that they have found and rendered passive many such attacks. Cyber Sabotage has reached to such an extent that superpower United States claims Russian Intervention in 2017 President Elections. Hackers also target installations like oil rigs, oil refineries, thermal power plant, nuclear power stations, dams etc. Attack on oil rigs may alter oil prices globally and may affect world economic balance. Attacks on nuclear power plants are very dangerous. Any country employs its best and sophisticated technologies in these infrastructures so any attack on them may reveal our best of technologies. Last year few media reports surfaced claiming cyber attack on Indian nuclear power plant but then government denied any such incident claiming that quick countermeasures were taken.

With advancement in space research, developed countries use space based systems for battlefield and espionage. This makes them a very fruitful target. Any attack damaging space infrastructure of a country will harm it to such an extent that damage control would take years to finally occur and till then technological development of that nation may be affected.

Cyber Espionage:

Beside this cyber attacks are used largely for espionage. Military installations, defense infrastructures are attacked in order to gain sensitive information. Some reports claimed that US PENTAGON was attacked by cyber means and much sensitive information was extracted. It was claimed that information regarding Joint Strike Fighter (F-35), F-16 Viper ,modernization of US Nuclear arsenal and about various other modernizations schemes were stolen by the hackers.

Chinese hackers and Russian hackers were claimed to responsible for the same. After reports of defector Edward Snowden, US were highly criticized for espionage under its

PATRIOT ACT. Reports claim that US tracked and tapped phone calls of different nations and also carried out illegal personal data collections of people of various nations.

Cyber /Psychological aspect:

Cyber propaganda is very integral part of both psychological and cyber warfare. Fake news sites are used to spread lies and propaganda. Doctored news and other means are employed to downgrade a particular nation in order to spread fear and terror. Terrorist organizations mostly use it to brainwash people. Our neighbour Pakistan employs it against us where its ISPR vomits only lies about use as we saw on 27th Feb 2019 where they claimed 2 IAF fighters to be shot but we know that only one was shot down . Furthermore they never acknowledged kill of their F-16.

Cyber War and India:

Owing to the changes in dimensions of war India must also change accordingly. Till 2016 we paid less attention in this area but now we have understood its importance. With establishment of Space and Cyber command I believe that our armed forces will join hands to fight heroically in this battlefield also. We must develop both offensive and defensive capabilities to act accordingly in any situation. Furthermore government should plan out structure of the command and its annual budget. We must understand that cyber warfare is equally dangerous as nuclear warfare, so our government and armed forces in close coordination must develop working principles and doctrines for the same and plan out our tactics and training keeping in mind requirement of present and future scenarios.