Cyber Security in India

Vijay Chauhan
Student, Dept. of Computational Science, Brainware University, West Bengal, India
vijaychauhan543@gmail.com

Abstract

ARPANET was developed by the US Military for a computer to computer communication between various US Defence Research establishments and Laboratories. Further, development of an advanced form of quick communication between the various authorities led the world to step into the first kind of digital age. But as the saying goes "Every action has an equal and opposite reaction" USSR responded by letting its premier spy agency KGB infiltrate the ARPANET and steal the researches of the US Military and it is said that they succeeded into it. Thus the concept of cyber security came into play and after it as the Internet went global more and more, countries began to join the fray of developing their cyberspace for their military and civilian uses. In the age of digitalization, cyberspace is now open for civil uses too rather than military only. But as things came with their pros and cons, Cybercrimes emerged as a potential challenge to deal with. In order to prevent the cybercrimes, civil or military infrastructure began to get digitalized. As regards the internet, the need for cyber security began to grow to protect the very interests of the nations. As the globalisation of the digital age grips the world major developed and developing nations, India is not far behind in this context.

Keywords: Cyberspace, Cybercrime, Cybersecurity, Cyberwarfare, Cyberattack.

Introduction

Objective of the study

To analyze the current cybercrime and cyber security situation in the country, its effects on India and its scope and future in India and the necessity of the skill development in the cyber security.

Research Methodology

Theory based mainly references from various websites and articles and analyzing the current scenario.

The first IT Act was passed in India in the year 2000 giving the country the legal framework for the proper and good use of the cyberspace but the need of a cybersecurity on the country wide infrastructure and creating cyber security experts and imparting skills of cybersecurity basis was something not emphasised much because the digitalization process was very slow in India and at that time the basic weapons for attacking one's individual or one country's cyberspace in the world was viruses, hacking of websites or malicious codes etc. but as the countries began to invest their resources of vital importances in the cyberspace and began connected to the internet of course for better governance and proper utilisation of Govt. capabilities for their countrymen's benefit boosting their economies and proper distribution of resources among the people over the point of time, it became an important arm of the country. The nation's interests began to rely on dangerous cyber weapons which were sophisticated and more target oriented in nature e.g. Adv worms and trojans, phishing, ransomwares, spywares etc. So, the cyber security became of utmost importance for protection of the nation's vital interests. In India before 2013 there was not a dedicated cyber security program in India by the Government.

Literature Survey

As the digitalization process began in India, the country's infrastructure began to grow and more and more people got access to the internet, the need for a cyber security policy was felt as the country infrastructure began to develop like the national power grid, automation of Indian Railways Signalling, the space program, ballistic missile programs and the last but not the least India's nuclear program. The digital governance system of the central government let all these programs run by the government for the betterment of the people and the proper distribution of the government resources for strengthening the country's infrastructure and boosting India's defensive capabilities as well as the economy of the country. The massive dependence on internet needed launching of cyber security at the national level in order to nullify the adverse activities in this context. Majority of the financial organisations are targeted by outsiders, organised crime groups etc. Recently Wannacry Ransomware attacks took place globally. India's Kudankulam Nuclear Power Plants was attacked but it was thwarted due to the air gap technology used to protect the main administrative computer in the plant but if the attackers have succeeded they would have stolen the valuable researches and the reactors designs. Kudankulam Nuclear Power plant is said to have an prototype nuclear reactor indigenously developed by our scientists. For any breach in the security of the nuclear power plant, the attacker can also stop the reactor or overload it leading to reactor meltdown. In both the cases it is said to have very disastrous consequences on the country. Over the time, the cyberspace has evolved into a 5^{th} domain of warfare. As the country ushers into the digital age and the number. of internet users are increasing, people are becoming more active on social media, digital media platforms, availing themselves of the digital governance. Most of them are vulnerable to the online threats as they have little to no knowledge of the threats of the internet so it is up to so social media, digital media companies need to develop a robust cyber security system. Side by side, the government should have a cyber security of their own by giving priority to the cyber security policy. India has growing economy, young population, over 250 data centres. Since all these are growing exponentially, the government must have tight robust and rigid cyber security systems to protect its citizens' interests. Apart from all these, India has a space program which is contributing to the national development. This agency is very active in the cyberspace and any breach in its security can cripple the national interests. NITI AAYOG, the Indian Govt. premier think tank agency has developed an outlook of the recent cyber attacks and the types of attacks the country is facing require proper classification depending on the dynamic natures of the attacks. The proper cyber security mechanism demands use of cutting edge technologies like the air gap tech, cryptographic algorithm for better data protection. As India is flexing its muscle against the cyber threats in its civil as well as in the military infrastructure, the cybersecurity capabilities of the Indian Armed Forces and the Central Securities Agencies is said to have developed significantly for protection of the nation's interests.

Conclusion

India is a developing nation. It has to develop and upgrade the cyber security infrastructure to tackle the threats . India has talented persons and emerging IT Sector from which it can draw its manpower domestically for protecting its cyberspace. Governments around the worlds should give priority to cyber security. India is a huge country with a huge population. India always has astonished major world powers in the field of defence. It is significant that the country will also do big in the cyber security field too with good governance. It has a potential to create history by benefitting the country as well as other developed and developing countries around the globe.

Future Scope

Research on this topic commonly stresses on making a cyber-warfare division to analyse the rising cyber threats and understand the dynamics of the nature of the threat emphasising on the type of attacks and identifying the type of potential attackers . Taking Israel, a cyber-secure country as a case study the needful defence-civilian partnership in the context of cyber security can explored. India has a huge IT market having millions of internet users surpassing US and giving competition to China but compared to these, cyber security experts happen to be less in number. So, focus should be on creating more cyber security experts and an adequate secure infrastructure. As said "Rome wasn't built in a day", for India it is a long way to go. India should focus on the future mastering the skills of cyber warfare and developing cutting edge technology along with its infrastructure.

References

[1] Cyber Security by Dr VK Sarasawat Member, NITI AAYOG a Govt of INDIA ThinkTank.

[2] Cyber Security in India: A Skill-Development Prespective by Ranjan Kumar, Niladri Mukherjee.

[3] "WION," *Wionews.com*. [Online]. Available: https://www.wionews.com

[4] "| NITI Aayog," *Niti.gov.in*, 2018. [Online]. Available: https://niti.gov.in/.

[5] "Quora - A place to share knowledge and better understand the world," *Quora.com*, 2019. [Online]. Available: https://www.quora.com/.

[6] "Wikipedia," *Wikipedia.org*, 2020. [Online]. Available: https://www.wikipedia.org/.