IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 11, November 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011074|

Cyber Warfare an Emerging Weapon of the 21st Century and the Biggest Non Violence Threat to a Nation

Dr.Sumanta Bhattacharya[1], Dr. Jayanta Kumar Ray [2], Shakti Sinha[3] , Bhavneet Kaur Sachdev[4]

Research Scholar at MAKAUT , Public–Foreign-Defence Policy Analyst , C.E , CH.E , CCIO , M.Tech , MA in Development Studies, LLB , M.A in Security and Defence Law , DIA&D , DG & GS , PGCPP & A , MPI(oxford University), India ORCID ID : 0000-0003-2563-2787[1]

National Research Professor, Ministry of Human Resource Development, GOI, Former Centenary Professor of International Relation, Department of History, CU, and Institute of Foreign Studies, CU and Honorary Consultant for Research in Indo-Bangladesh Relations, Kolkata, Former Chairman , Maulana Azad Kalam Azad Institute of Asian Studies, Kolkata, India[2]

Honorary Director, Atal Bihar Vajpayee Institute of Policy Research and International Studies, India[3]

Political Science hons (Calcutta University), Masters in Development Studies, India[4]

ABSTRACT: Cyber Warfare is the war of the 21st century which is a big threat to the world .India is not a superpower when it comes to cyber security . Cyber fraud and cyber warfare has gained momentum in the 21st century. India in 2019 was attacked by China 40,000 cyber attacks against India , Chinese attacked the Mumbai's electric grid and the train stopped all of a sudden , the main area of cyber attack is in Its and Banking sector of India . There is a cyber security policy existing in India since 2013 which has not been fully implemented , we see a rise in the cyber crime cases in India especially in 2020 with the lockdown taking place . India's data is being leaked .Apps such as Zoom and Tik Tok has been used to get access to India's internal data . India has a poor infrastructure , there are many agencies who are looking into the cyber world . However there is lack of skilled trainers in the cyber security field which calls for introduction of better training infrastructure and courses on cyber security to include more people and increase awareness .Cyber Forensic is also one of the ways by which we can stop cyber warfare and attack in India .

KEYWORDS : Cyber attack , cyber warfare , cyber security , Cyber Forensic , infrastructure , cyber fraud .

I. INTRODUCTION

With the advance in technology we see a bloom in the use of cyber space which would include computers , cell phone , Internet and other technology devices which has also resulted in an increase in cyber crimes . Cyber crime also be referred to as high technology crime or e-crime which makes the use of computer and internet .With rise in Cyber crime we also require cyber security which is emerging as a complex issue with an increase in multi-domains. Cyber space has expanded with the development in Information Technology (IT) and the commercial application . With a rise in information technology and communication , we see a rapid change in the science , education and commercial infrastructure . Today , in this modern era Information Technology plays a very significant role in the development of important infrastructure such as telecommunication , transport , energy , power , emergency , defence system , space , satellite , law enforcement , traffic control network , in the delivery of goods and services . , the stability and security of these data are very important for the economic security of the nation . Cyber warfare and cyber terror has acted as a threat to the security of a nation . Cyber crime can be an amalgamation of both online and offline crime . Cyber threats can be categorised into two groups : Cyber Crime that is against an individual or corporate or an organization, and the second is cyber warfare that is against a state . Further Cyber crimes can be classified into two groups , Crimes that Target computers directly which incorporates Spreading computer viruses ,Denial-of-Services (DoS) an attack which restrict the users from getting access to its own resources , Malware – is a software that used to destruct computer applications to gather information , or get access to private computer systems , for example Trojan Horse , worms , rootkits are examples of such software which can appear in the form of codes , active content or scripts. And the second

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011074|

kind of cyber crime includes rimes facilitated by Computer Networks or Devices , the basic target of which is independent of the computer device which includes economic frauds which is use to destabilise the economy of a country , extract money through fraud , debit and credit card fraud . financial theft , attack on banking transaction , phishing scams , misuse of social media platform , threatening e-mail , copyright infringement , cyber stalking , threatening girls , cyber blackmailing , spreading obscene content , spreading pornography , fake job offers , creating fake identity and accounts , Breach of right of privacy are some of the examples of cyber crime . They key terms of Cyber Attack would include Phishing , Vishing , Tabnapping , Whaling , Spoofing , Zombies , Botnets , PHARMING , Drive-by , MITM and Spam . However the most come is hacking and identity theft which is emerging as a threat to India 's cyber space.

II. RESEARCH METHODOLOGY

For the purpose of this exploration , I have used a amalgamation of two of the archetypical social sciences research tools application –as they are authentic and brilliant method to assemble statistics from multiple appellant in an methodical and convenient way . Question were asked to the parents and their children , survey , interviews –consisting of several interrogation which were dispersed among representative of each contender group.

Objective of Research

In this Research paper the main area of studies include

1.What is cyber warfare and cyber crime

2. Types of cyber crime and cyber warfare activities and how it has affected India.

3.Cases of cyber attack and cyber terror in India .

4. What has the government done to strength cyber security in India .

5. What is the future perspective of cyber warfare in India .

III. LITERATURE REVIEW

Cyber warfare can be defined as an initiative taken by the state to sabotage and espionage against another nation using internet as a weapon . Attacking the information of another state for espionage and for disrupting the critical infrastructure . It may include hacking a website , important website , strategic controls and intelligence . Cyber warfare is practised by many states and individual organization and terrorist groups to gather information and hack a website which is referred to as cyber terror , Cyber warfare has its own characteristics which is very different from the traditional warfare : Independent theatre of war – The development of internet and growth of these wireless communication is used in various economic , social and political transactions and purpose , these technologies play an important role in military operations , navy , land , air and now in space also ,internet has been now used by many states to prefer aggressive activities , use by criminals and terrorist groups ,Cyber space has been regarded as the fifth potential threat to war after land , air , space and sea . They use of cyber space depends on physical provisions like microwave , telecom exchange , undersea , cables , routers protecting them is the duty of traditional arms of military .
An undefined space Cyber space has a special feature they are not defined like in the case of land , sea and air forces there is a specific area which is defined .The outer space and cyber space are different , moreover the global internet space is under the authority of one country , so in order to protect one's cyber space national cooperation and defence security needs to be maintained .

Disguised Attackers: In cyber space a person can easily mislead his target into believing that the attack has come from somewhere else, it becomes very difficult to identify the attack , which makes the design of security structures and policies very complicated compared to other threat of conflict .
No Contact War : The evolution of technology impacts and the nature of conflict and war , in cyber space there is no contact war and there is no physical action across the borders and the world war will become more like a cyber war .
Cyber space has become vulnerable to cyber attacks and crime , cyberspace has no geographical boundaries or limitation which makes it more challenging , India has been a victim of cyber attacks in the recent past , on the other hand we depend on cyber spaces for a number of purpose from Booking tickets , transferring money , nuclear power facilities, power transmission which has resulted in rapid economic growth and development . Cyber attacks are of four types : Cyber Espionage , Cyber Attack , Cyber Terrorism and Cyber warfare , India is the third most vulnerable country to cyber attacks as per the report of Internet Security Threat .

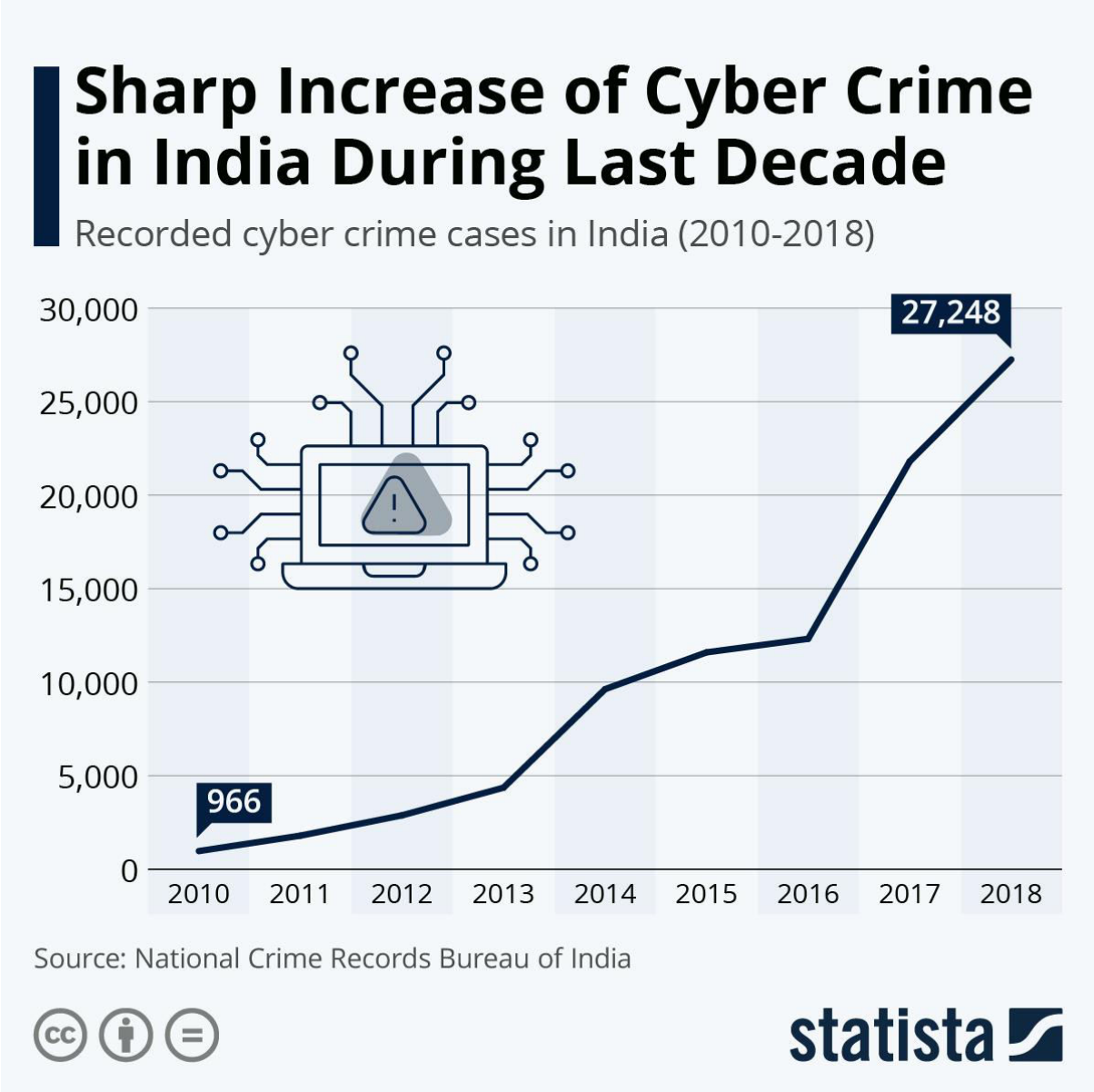
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011074|

IV. FINDINGS

In 2017 the WannaCry and Petya Ransomware attack , In 2018 we had the aadhar software getting hacked details which resulted in the leak of details online . From 2016 to 2018 , India was the second most cyber attacks affected country . 1.25 Lakh rupees was lot in 2019 due to cyber crime in India. Cyber Espionage is the practice of gaining information that is sensitive , personal , categorised nature from individuals to administration using vengeful software like Trojan Horse , the aim is get access to confidential facts which will go against the Homeland Security . Cyber charge – mainly choose PC , computerized structures , infrastructure , PC grid to cause problem or damage chosen computer networks or structure , Demolition of connecting networks , Cyber warfare , Meshwork has been used by terrorist for a number reasons like designing terrorist attacks , mobilize of sympathizers , raise funds and to modify people .Cyber warfare- Cyber warfare basically includes carrying out warfare by using computer system by one country to attack the computer system of other country which incorporates theft , destruction of critical information infrastructure and vandalism.



Cyber warfare has a greater impact on important information infrastructure , majority of the sectors rely on ICT for their everyday work , these sectors would incorporate the banking and finance , transportation , telecommunication , power system . Cyber hacking on these sensitive material infrastructure caneffect the country security and system in a matter of seconds. Chinese Cyber attack in Mumbai on the power system changed the scenario of the country , the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011074|

local trains stopped functioning and people git stranded . Cyber attack affects the national security and stability of a country .

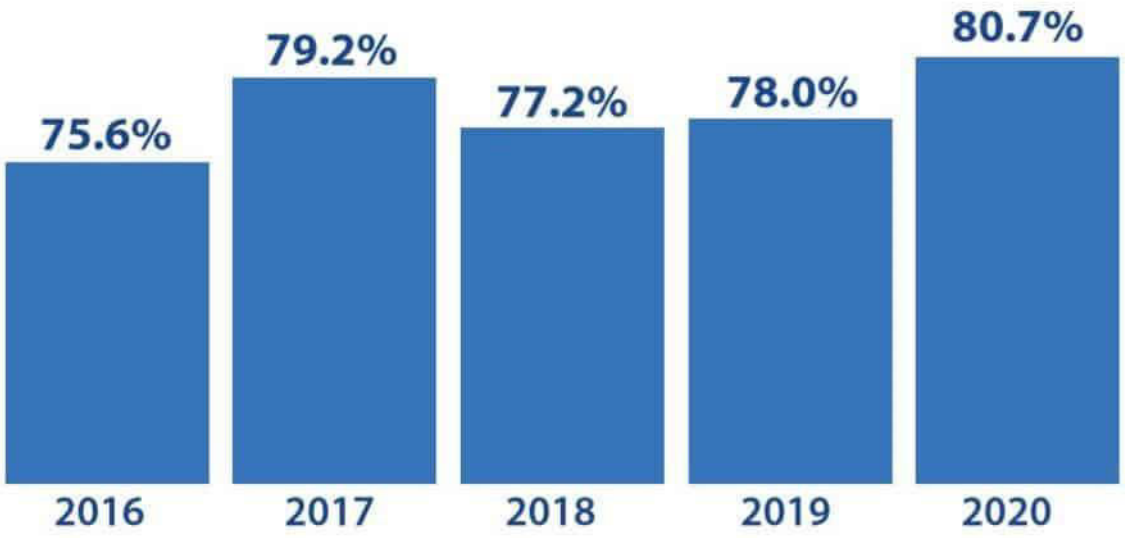


Figure 2: Percentage compromised by at least one successful attack, by year.

India's cyber space is not protected and we have lack of ICT infrastructure , the crucial areas of targets become the defence installations , ATC management , Financial services , railway traffic control , communication networks, including satellites, sensitive data related to both internal and external security and premier institution of science , technology and research . The government of India has taken many steps to improve the cyber security of India by recognising a list of sensitive computer structures which requires security against cyber crime such as line of network related to defence , banks , stock market , power grid national security , railways and airlines weather . In 2013 , a national policy on cyber security was framed , A national Critical Information Infrastructure Protection Centre (NCCIPC) was formed to built a full verified firewall surrounding these systemto enhance the security and elasticity of the country's analyticdata , a cross -agency National Cyber Collaboration Centre was created to provide reports on cyber threats and allocate information with main stakeholders , centre of excellence in Cryptology , the science of encoding data was established at the Indian Institute of Statistics of Kolkata . A roadmap on cyber security was laid down in collaboration between the government and the private sector , CERT-In or computer emergency response team (India) was set up to deal with such catastrophe on a diminutive level for specific areas , the army had established CERT for themselves and the railway and power zone also established CERT later on its function is to respond to computer security incidents . A cyber crisis management plan was set up with state government playing an important role with the objective to counter cyber threats and cyber terrorism . National Cyber Safeguard Coordination (NCSC) under the National Security Council Secretariat collaborates with various organization at the national level for cyber safety affairs , Cyber Surakshit Bharat Initiative was introduced in 2018 with the objective to share consciousness on cyber crime and institution building to compute for principal knowledge security officers(CISOs) and IT staffs across all administration agencies and Information Security Education and Awareness Project (ISEA) - -it was formed to supply awareness , pedagogy , research and training in the sector of data security .

International Accord : Presently , Budapest Convention is considered to be the first international agreement to give importance to the crimes related to internet and cyber by harmonizing laws , enhancing investigation and collaboration within nations .This accord provides greater collaboration protection against cyber crimes , India is not part of this accord , as it grant access to data across borders which India thinks this might infringe on National Sovereignty .

PPP infrastructure for data security – In India most of the cyber safety work is carried out by the administration agencies such as CERT-In , with speedy exchange nature and increase in cyber challenges , we have to anchorage private actors in fighting cybercrimes through PPP model

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011074|

Experienced professionals –India requires 10 lakh cyber security experts according to NASSCOM , at present there are only 64,000 professionals , this is because of the lack of courses available in the field of cyber security , lack of training facilities and infrastructure results in lack of trainers .Make strong and strengthen IT act and national security policy 2013- The present cyber security framework and IT act are old and not equipped enough to stand the advanced cyber crimes.

V. FUTURE PERSPECTIVE

Lockdown saw a massive rise in cyber crime cases , two moths cases reported was equal to 10 years of cases reported in the past years . Cyber crime has amplified with time since the 2000s with the advance in technology which has promoted cyber warfare around the global which affects the economic , attack major banks and data of a country's which can change the scenario in no time . India has experienced cases of cyber terror in the past few years

COMMON METHODS OF TARGETTING

Major types of crimes	Jan	Feb	March	April
Debit/credit card frauds (vishing)	87	141	347	202
Job fraud	8	27	41	9
Card skimming	47	56	83	10
Gifts and loan offers	49	102	209	38
Social media cases	23	35	57	52
Other advance fee scams	10	8	12	7
Business opportunity fraud	3	15	11	4
Total	305	490	878	430

The Zoom which is being used by maximum number of companies and institution to organize classes and meeting actually didn't have security and most of the data was being leaked of the government and of many organization which has emerged as a threat for the nation. Cyber Forensic can help in limit cyber warfare in a few ways .For instance If the laptop/computer used for criminal purpose has been seized, the analysis of the device using forensic tool will help to understand the nature of crime and analyze other data such as history of browsing websites, traces of using malware software etc. which may give the trace of the criminal.The authentication of Email forensically will help us to confirm the actual source of the email. It will prevent us from becoming the victim of phishing, The authentication of audio, video and images using forensic tool help us to check whether there is any tampering or editing in the files, the forensic tools can help to recover the deleted data from mobile phone, hard drive or other memory devices and Cyber forensic provide security to the important data stored in a system. We also need to introduce cyber infrastructure development program and courses to train people in cyber security .

V. CONCLUSION

India doesn't have a strong cyber security system thought the government in 2013 had introduced the cyber security policy in which there are many policies which have not been implemented . Many agencies have been formed for the protection of cyber terror , where all the data is shared between different agencies and Ministry and on a daily based information is exchange . The government has also signed many pact with their neighbours and other countries , introduced by India in the protection and preservation of data from been leaked .

It has a critical impact on the infrastructure , India has a poor cyber infrastructure which requires development by providing training and or organising course on cyber security increasing the knowledge among the people on cyber and

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011074|

its threat ,Cyber crime is the new era war which is weapon less and more harmful than other forms of war . Cyber Terror has gained momentum since 2019 with complete lockdown , every 5 minute a cyber crime is being reported across the country . Cyber Terror in present time can be seen in the form of apps by which data is being leaked with no security .In 2019 there has been 40,000 cyber attacks from China in India on the IT and banking sector .

REFERENCES

1.Shristi Deoras ,2021 , Can India Stand up to China's Cyber warfare .
2. Cyber warfare , DSCI.
3.Manjari Chatterjee Miller and Engine Kirda , The growing threat of cyber warfare .
4.Nikhil Ramphal , 2020 , September , India is no superpower in Cyber space .
5.ASIA-PACIFIC , Military standoff apart India, China brace up for cyber –warfare .
6.Deepak Vohra , 2021 , March ,China launches warfare against India .
7.Robinson M , Jones K , Janicke H , 2015 , March , Cyber Warfare : Issues and Challenges , Computer & Security .
8.Mukherjee Sourav , 2019 , July , Cyber Warfare and Implications , SSRN .
9.Maurice Eugene Dawson Jr ,2000, Cyber warfare : Threats and Opportunities .
10.Yuchong Li , Qinghui Liu , 2021 , September , A Comprehensive Review study of cyber-attacks and cyber security ; Emerging trends and recent developments , Energy Reports .

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details