International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

A Study on National Cyber Security

S.Sibbhi Raj, Dr. B. Lavaraju

Saveetha school of law, saveetha institute of medical and technical science (simats), saveetha university, chennai -600077

M.com., llm., ph.d., associate professor, saveetha school of law, saveetha institute of medical and technical sciences, saveetha university, Chennai – 600077

Date of Submission: 08-05-2023 Date of Acceptance: 20-05-2023

ABSTRACT

Cybersecurity has become a complex and fast-moving security challenge in the age of Information Communication and Technology (ICT). As the dependence on ICT is deepening across the globe, cyberthreats appear likely to penetrate every nook and corner of national economies and infrastructure; indeed, the growing dependence on computers and Internet- based networking has been accompanied by increased cyberattack incidents around the world, targeting individuals, businesses, and governments. Meanwhile, ICT is increasingly being seen by some governments as both a strategic asset to be exploited for the purposes of national security and as a battlefield where strategic conflicts can be fought The objective of the study is to To build a secure and resilient cyberspace for citizens, businesses and Government. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment. To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem. The independent variables are age, gender. ,occupation. The dependent variables are performance metrics does the government have for the strategy in cyber terrorism. Does the criminal law adequately address offenses committed online. The total no of responses are 200. This paper examines the primacy of cybersecurity in the contemporary security debate, deepening the analysis by looking at the domain of cybersecurity from the perspective of India.

KEYWORDS: Cyber security, Cyber Space, Human Rights, National threat, Terrorism.

I. INTRODUCTION:

The concept of security is a core concept in the study of international relations. Traditionally, and until relatively recently, security analysis focused on state security, viewing it as a function of the levels of threats which states face from other states, as well as the manner and effectiveness of state responses to such threats. However, after the end of the Cold War, scholars shifted focus from the state-centric notion of security, enlarging the concept to include the protection of the individual.**("Cyber Security Objectives" 2012)** At approximately the same time, the nature of threats changed from external aggression to intra-state conflicts arising due to civil wars, environmental degradation, economic deprivation, and human rights violation. It is in this context that national security came to include within its ambit other issues of security apart from territorial protection, such as poverty, industrial competitiveness, educational crises, environmental hazards, drug and human trafficking, and resource shortages**(Lobato, n.d.).** Finally, the recent Information, Communication and Technology (ICT) revolution — including the Internet, email, social websites, and satellite communications — has revolutionised every aspect of human life, posing new challenges to national security. Indeed, in the digital age, the arena of national security is confronted with previously unfamiliar threats aimed at destroying a state's technology infrastructure. It is an obvious truism that, in the globalized world, the Internet and ICTs are essential for economic and social development, forming a vital digital infrastructure upon which societies, economies, and governments rely to perform their essential functions. The relatively open nature of the Internet guarantees that it is, on numerous levels, an unsafe environment.**(Lobato, n.d.; Shinde 2021)** As such, cybersecurity has come to encompass a wide range of issues such as critical infrastructure protection, cyberterrorism, cyberthreats, privacy issues, cybercrime, and cyberwarfare.In the second decade of the twenty-first century, cyberthreats are evolving and increasing at a fast pace. They are still

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

initiated by criminal actors but also come from new sources, such as foreign states and political groups, and may have motivations other than money making. These latter may include some types of "hacktivism" in the name of a political cause, political destabilisation , cyberespionage, sabotage (e.g., Stuxnet), and even military operations **(Lobato, n.d.; Shinde 2021; Graham, Olson, and Howard 2016).** The sophistication of cybercriminals, the emergence of cyberespionage, as well as the well-publicised activities of hacker collectives have combined to create the impression that cyberattacks are becoming more organised and that the degree of sophistication has increased significantly, showing clear signs of professionalisation.(Lobato, n.d.; Shinde 2021; Graham, Olson, and Howard 2016; Shukla and Agrawal 2020). The main aim of the research paper is to discuss about the cyber terrorism and its impact in India.

II. OBJECTIVES OF THE STUDY:

The objectives of the present study are as follows

1)To build a secure and resilient cyberspace for citizens, businesses and Government.

2)To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment.

3)To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4)To prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structure.

III. REVIEW OF LITERATURE:

Network outages, computer viruses, data conceded by hackers, and other incidents affect our lives in ways that range from troublesome to life-threatening, as most government and financial institutions, military groups, corporations, hospitals, and other businesses store and process an abundant deal of confidential information on computers**.(Ambika, Ambika, and Senthilvel 2020)** Thus, with the increasing volume and sophistication of cyberattacks, there is an increased need to protect personal information and sensitive business as well as to safeguard national security.Accordingly, the term "cybersecurity" refers to the collection of tools, policies, guidelines, training, actions, security concepts and safeguards, risk management approaches, assurance, and technologies that can be used to secure and protect the cyber environment as well as organisation and user assets(Ambika, Ambika, and Senthilvel 2020; **"Cyber Victimization of Women and Cyber Laws in India," n.d.).**In addition, cybersecurity aims to secure information technology and focuses on protecting computer programs, networks, and data, along with preventing access to information by unauthorised users as well as preventing unintended change or intended/unintended destruction**(Ambika, Ambika, and Senthilvel 2020;** "Cyber Victimization of Women and Cyber Laws in India," n.d.; Gupta and Rao 2007).Furthermore, cybersecurity plays a vital role in the ongoing development of information technology and Internet services. In the process, state security and countries' economic well-being have become increasingly reliant upon the successful protection of critical information infrastructures. Consequently, in many countries, making the Internet as safe as possible is now integral to the development of government policy as well as new services. The rest of this article examines the extent to which India has, to date, successfully dealt with this emergent challenge. In the Indian context, the issue of cybersecurity has received relatively little attention from policymakers, to the extent that the government has been unable to tackle the country's growing needs for a robust cybersecurity apparatus**(Dasgupta 2009).** In short, India lacks effective offensive and defensive cybersecurity capabilities, exacerbated by the lack of access to mechanisms vital to confronting sophisticated malware like Stuxnet, Flame, and Black shades. Moreover, cybersecurity projects and initiatives in India are far fewer in number as compared to other developed nations. Many of the relevant projects proposed by the Indian government have remained on paper only**(Dasgupta 2009; Patil 2021).** In addition, approved projects like the National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) of India have failed so far to materialize. Worse, the 2013 National Cyber Security Policy of India has failed to bear fruitful results, as its implementation seems to be weak in numerous aspects, including privacy violation in general and intrusion into civil liberties in particular**(Dasgupta 2009; Patil 2021; Sharma 2017)**. The IT sector in India has emerged as one of the most significant catalysts for the country's economic growth, and as an integral part of the country's business and governance. The sector is positively influencing the lives of Indian citizens through direct or indirect contribution to the improvement of several socio-economic parameters, such as the standard of living, employment, and diversity. In addition, IT

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

has played a key role in transforming India into a global player in providing business services as well as world-class technology solutions**(Dasgupta 2009; Patil 2021; Sharma 2017; Ariely 2007)** .At the same time, the growth of the IT sphere has been accompanied by a tremendous and increasing need to secure the computing environment, as well as the necessity to build adequate confidence and trust in this sector . For example, most financial institutions as well as the banking industry have incorporated IT in their operations, opening up countless opportunities for growth while at the same time making these institutions vulnerable to cyberattacks in their daily activities and making the evident absence of strategies to deal with these types of threats particularly worrisom. Securing the energy sector has emerged as a critical non-traditional security issue for India. The country ranks fourth in the world in terms of primary energy consumption; at the same time, the average level of consumption per capita is very low**(Cohen 2014)** .Due to insufficient regulation of information sharing and incomplete institutions to facilitate it, information on cyberattacks and equipment vulnerabilities in the Indian energy sector is nearly non-existent**(Cohen 2014; Elliott 2002).** But we can suppose from trends in international cybersecurity that the sector is increasingly targeted by the sophisticated attacks, particularly as India has embarked on linking it with modern technologies in order to meet growing energy needs Indeed, with the advent of new technologies in this sector, several challenges began to appear on the scene**(Cohen 2014; Elliott 2002; Ullah 2017).** For instance, after India's nuclear test in May 1998, a group of hackers posted anti-India and anti-nuclear messages on the website of Bhabha Atomic Research Center (BARC) In addition, an online hacker called Phr OzenMyst hacked the official website of BARC and leaked some of its sensitive information; the attack was meant as a protest against ongoing government operations in the occupied part of Kashmir .Furthermore, the critical infrastructure supporting every economic activity in India is fully dependent on the power sector; the dependence of this sector on ICT has highlighted several cybersecurity challenges**(Clarke and Knake 2010)**. It is estimated that the period from 1994 to 2004 witnessed around 60 percent of all cyberattacks on the automatic power grids in India More recently, on July 30 and 31 2012, northern India witnessed a severe blackout that affected nearly 670 million people's normal life and work ,damaging all services in the region, including road traffic and railways. Chaos broke out on the roads as traffic lights and systems that supported them stopped working, with the police unable to cope with the situation**(Clarke and Knake 2010; Jarmon and Yannakogeorgos 2018).** Simultaneously, there were reports of devastating fires and explosions in major refineries, with extensive damage and loss of life, all while pipelines were ruptured and oil flow was disrupted .India has an extensive defence industrial base and maintains the third-largest armed forces in the world**(Richards 2014)** .At the same time, it has linked its defence sector with the new technologies, in the process opening the country up to a set of ever-evolving threats due to a dependence on these technologies and the reliance on integrating networks. For instance, in 2012 a cyberattack was launched by hackers against the Indian Navy's eastern command computer systems which oversee the testing of India's ballistic missile submarines and maritime activities in the South China Sea**(Richards 2014; "Cyber Security Threat Actors" 2016).** The naval computers were infected by a virus that secretly collected confidential documents and files and transmitted them to Chinese IP addresses.While Indian officials have yet to disclose the type of information that was targeted in this attack ,the Navy is not the only Indian defence institution to have faced such adverse events — the National Security Agency (NSA) and the Air Force have proved to be vulnerable as well. In 2010 the hackers targeted the NSA's office as well as several computers of the Indian Air Force, opening up numerous small windows through which classified files and documents were stolen **(Stratton 2009).** In the same year, the country witnessed the biggest cyberattack yet, in which more than 10,000 email addresses of the top government officials were hacked, particularly military officials, the Prime Minister's Office (PMO), defence, home ministries, external affairs, and intelligence agencies.

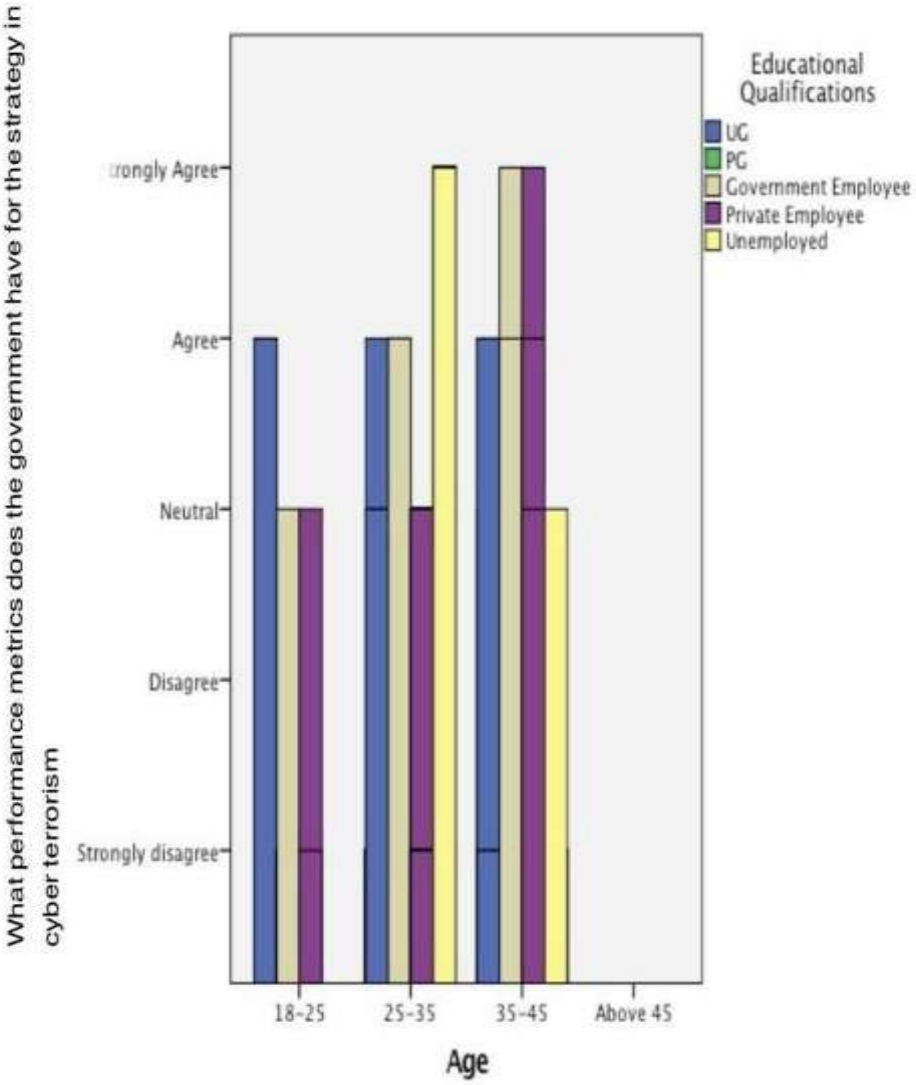
IV. MATERIALS AND METHODS:

The present research is based on empirical study and this research is made in Analytical and descriptive form in a science that the issues have been resolved into Elements and the structure of the issues has been described and classified. This is widely used in social research and also in legal research form. The source of Information is from the primary sources which are gathered as a result of survey Questions and by reference of certain books and other such journal articles. In a Random Method about 200 samples were collected for this survey. The sampling method was a random sampling method. The independent variables are

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

based on the sample's Age, Gender, Qualification and Occupation. The dependent variables are based on the questions: 1.What performance metrics does the government have for the strategy in cyber terrorism. 2. Does the criminal law adequately address offenses committed online?

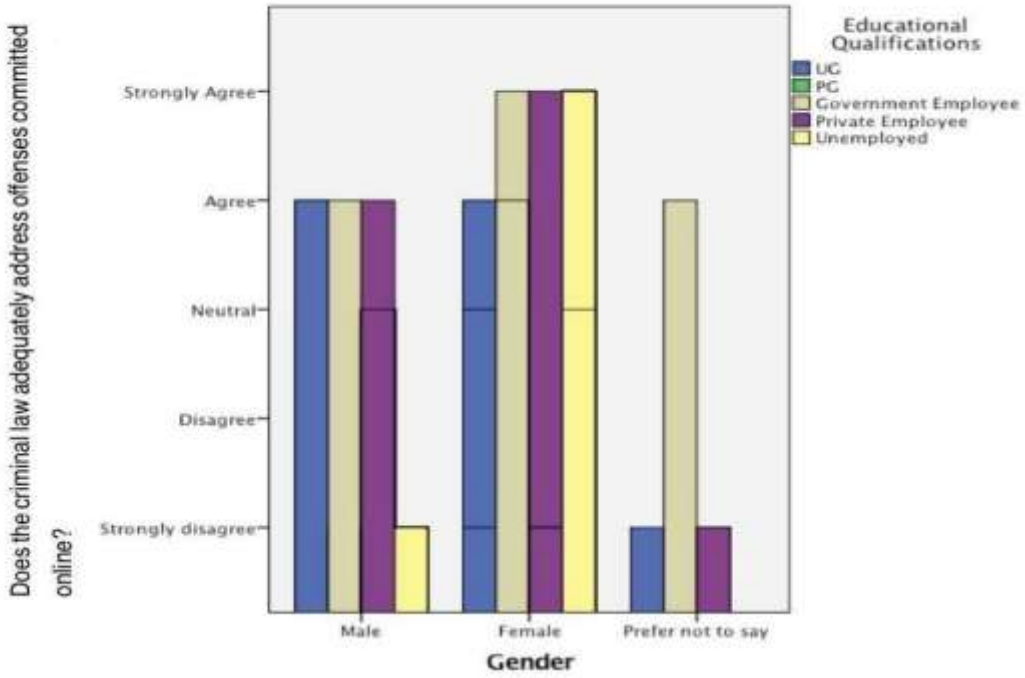
4.1. ANALYSIS AND DISCUSSION:
FIGURE:1



LEGEND:
The figure 1 defines the relation between age and educational qualification of the respondent across Chennai and their opinion on performance of the government for the strategy in cyber terrorism.

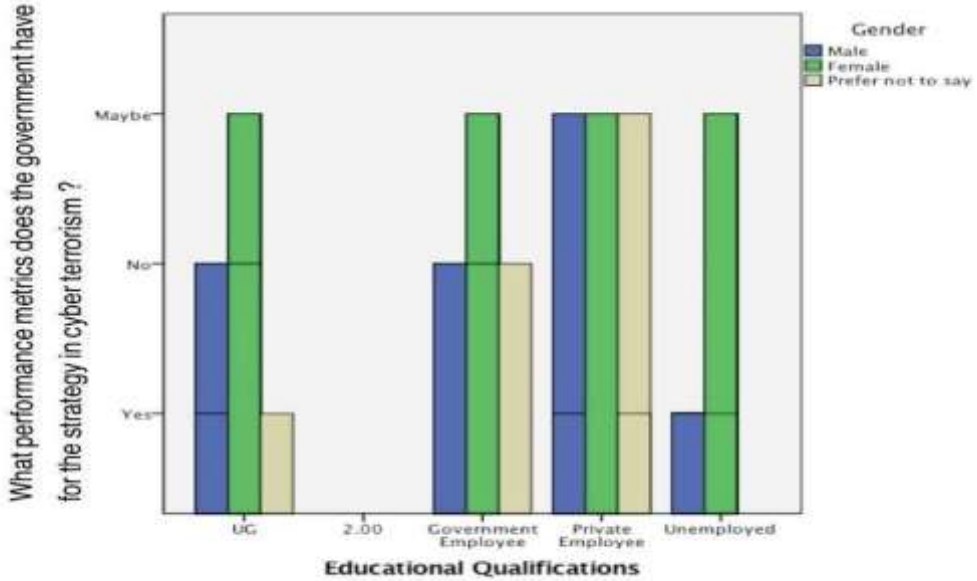
International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

FIGURE :2



Legend:
The figure 2 represents the bar chart of gender and educational qualification across Chennai and their opinion on criminal law adequately address offences committed online.

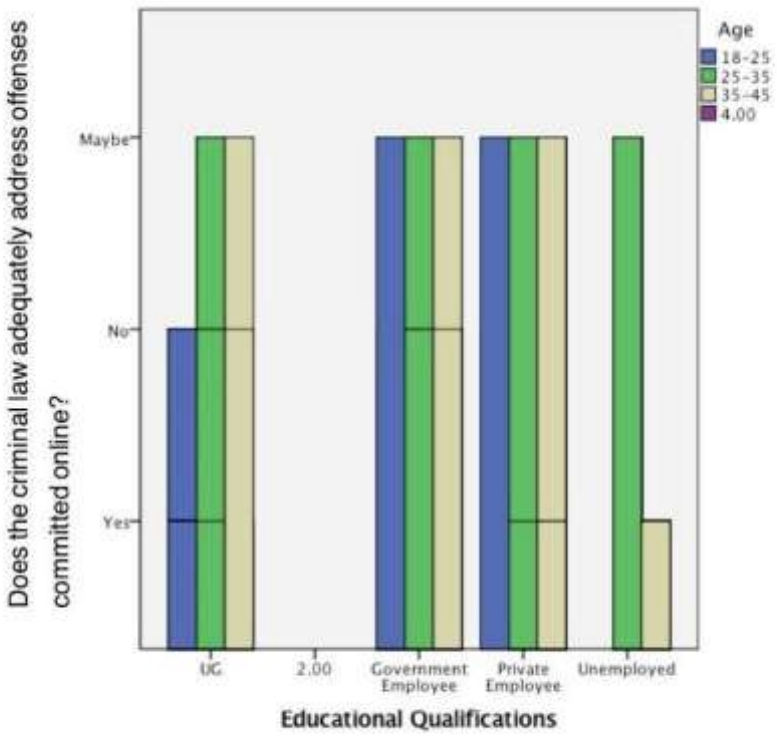
FIGURE:3



International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

Legend:
The figure 3 represents the bar graph of education qualifications based on gender in performance of the government for the strategy in cyber terrorism.

FIGURE: 4



Legend:
The figure 4 represents the analysis of educational qualification with age of the respondents for the criminal law adequately address offences committed in online.

V. RESULTS:

Figure 1: From the figure,it is revealed that age has a very vital influence on public response regarding performance of the government in making strategy of cyber terrorism . From the result it is clearly seen that age of the person on the basis of their educational qualification shows their opinion varies from one to another.

Figure 2: From the figure, it is found that there is a significant change between independent and dependent variables.Because criminal law adequately addresses the offences even committed online . In the case of gender with the educational qualification female opinion varies from male respondents, it shows that women's respondents' opinion given high interest over male respondents.

Figure 3: From the figure , it is revealed that educational qualification has a very important role in public opinion on the performance of the government in making strategies on national security threats. From the gender of the respondents there is significant change in opinion.

Figure 4: From the figure, it is found that relation between dependent and independent variables. The age with educational qualification shows the significance of the respondents on their opinion. And the opinion of the respondents in government and private employees are similar to each other.

VI. DISCUSSION:

In fig. 1 on an average people in the age category of 25-35 and 35-45 had given their opinion as strongly agreed as performance of the government in making strategy in cyber terrorism.In fig.2 on an average, respondents from gender with educational qualifications categorised as others and belonging to females have stated that there is greater effectiveness, this may be due to the

reason that people from that category are aware about the conditions of this provision. In fig.3 respondents had given highest respondents and its is to be the prominent opinion over males opinion. This may be due to awareness of the situation in practical aspects. In fig.4 with analysis of educational qualification with age in the category of government and private employees are similar and opinions are given equal based on educational matters.

VII. LIMITATION OF THE STUDY:

The research is done using empirical research methods through e-survey due to COVID-19 restrictions. The restrictive area of the sample size is the major drawback. The physical factors are not impactful and are not a major factor limiting the study as the present study is with online response. Moreover, the sample frame is also a limitation. The sample frame is Chennai which is having no specific reference.

VIII. SUGGESTIONS:

Conclusions When a country develops its cyber security strategies at national or federal level, it is a very difficult question what issues are covered by the specific strategy, how and in what form it is intended to address cyber-challenges. In accordance with the above-mentioned difficulties it is necessary to take into account the recommendations made by the international organizations, which can serve as a basis for building a country's national cyber security strategy and its key regulatory issues. This enables the possibility that, although the countries at national level form a cyber security strategy, they can still be in line with each other, with the same philosophical background, and thus more or less independent of the strategic ideas that are in the same direction from the interests and values of the given country.

IX. CONCLUSION:

As the preceding pages make clear, cyberattacks targeting critical information infrastructures in India, such as energy, financial services, defence, and telecommunications, have the potential of adversely impacting upon the nation's economy and public safety. From the perspective of national security, the securing of the critical information infrastructure has become a top priority, in line with policies already adopted by other digital nations. Indeed, the ever-growing interdependence of the digital sphere, across borders, has provoked the emergence of cybersecurity as a major component of national security strategies in states across the globe ; India should not delay in following their example.

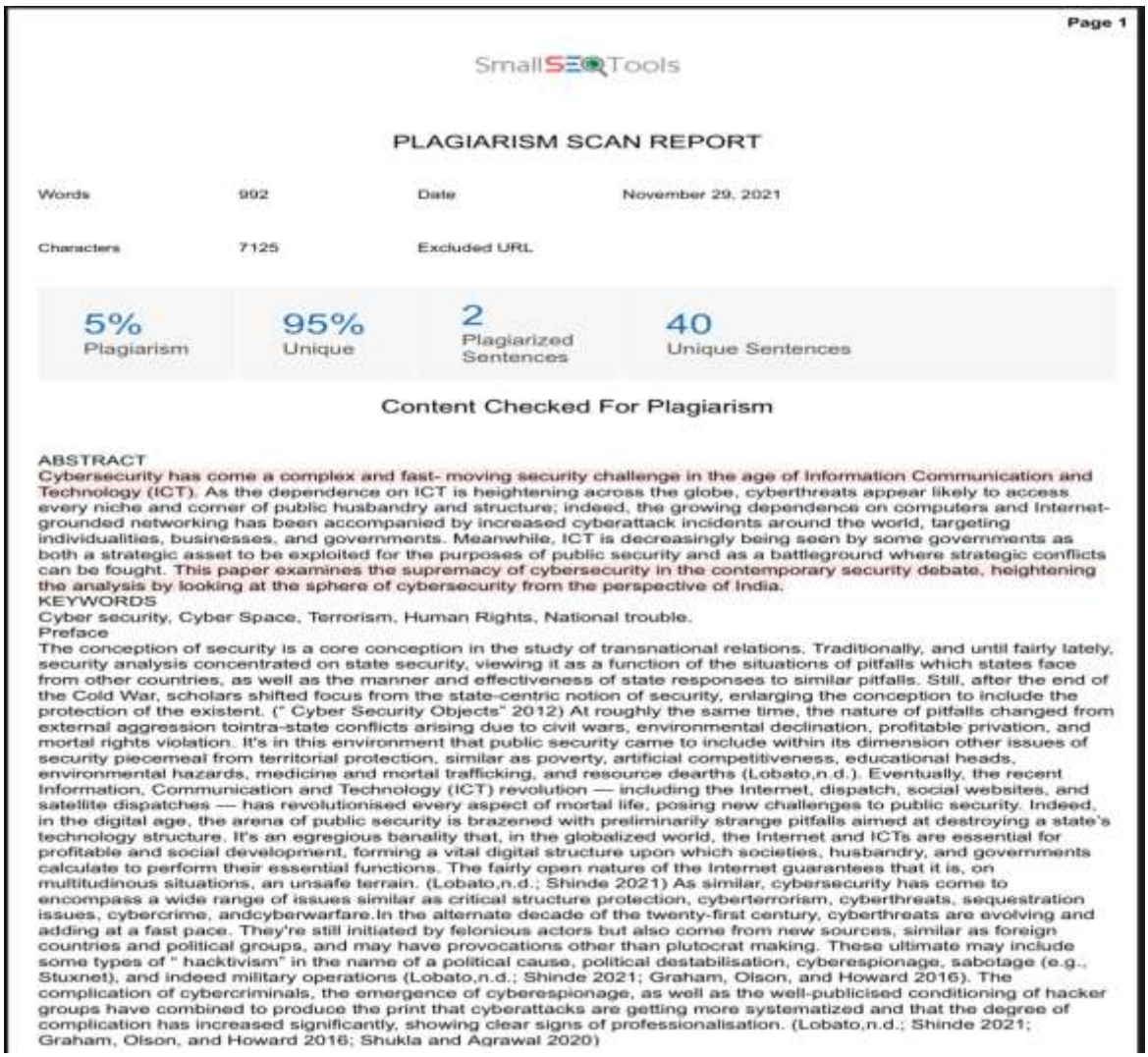
REFERENCES:

1) Ambika, Dr T., T. Ambika, and K. Senthilvel. 2020. "Cyber Crimes against the State: A Study on Cyber Terrorism in India." Webology. https://doi.org/10.14704/web/v17i2/web17016.
2) Ariely, Gil. 2007. "Knowledge Management, Terrorism, and Cyber Terrorism." Cyber Warfare and Cyber Terrorism. https://doi.org/10.4018/978-1-59140-991-5.ch002.
3) Clarke, Richard A., and Robert Knake. 2010. Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins.
4) Cohen, Daniel. 2014. "Cyber Terrorism." Cyber Crime and Cyber Terrorism Investigator's Handbook. https://doi.org/10.1016/b978-0-12-800743-3.00013-x.
5) "Cyber Security Objectives." 2012. Cyber Security Policy Guidebook. https://doi.org/10.1002/9781118241530.ch3.
6) "Cyber Security Threat Actors." 2016. Cyber Crime, Security and Digital Intelligence. https://doi.org/10.4324/9781315575667-15.
7) "Cyber Victimization of Women and Cyber Laws in India." n.d. Cyber Crime and the Victimization of Women. https://doi.org/10.4018/978-1-60960-830-9.ch009.
8) Dasgupta, M. 2009. Cyber Crime in India: A Comparative Study.
9) Elliott, Joyce E. 2002. "Cyber Terrorism: A Threat to National Security." https://doi.org/10.21236/ada404381.
10) Graham, James, Ryan Olson, and Rick Howard. 2016. Cyber Security Essentials. CRC Press.
11) Gupta, Manish, and H. R. Rao. 2007. "Role of FS-ISAC in Countering Cyber Terrorism." Cyber Warfare and Cyber Terrorism. https://doi.org/10.4018/978-1-59140-991-5.ch011.
12) Jarmon, Jack A., and Pano Yannakogeorgos. 2018. The Cyber Threat and Globalization: The Impact on U.S. National and International Security. Rowman & Littlefield.
13) Lobato, Luísa Cruz. n.d. "UNRAVELING

THE CYBER SECURITY MARKET: THE STRUGGLES AMONG CYBER SECURITY COMPANIES AND THE PRODUCTION OF CYBER (IN)SECURITY." https://doi.org/10.17771/pucrio.acad.27784.

14) Patil, Sameer. 2021. Securing India in the Cyber Era. Routledge Chapman & Hall.
15) Richards, Julian. 2014. "Responses to the Threat: National Cyber Security Planning." Cyber-War. https://doi.org/10.1057/9781137399625_5.
16) Sharma, Nishesh. 2017. Cyber Forensics in India: A Legal Perspective. Universal Law Publishing.
17) Shinde, Anand. 2021. Introduction to Cyber Security: Guide to the World of Cyber Security. Notion Press.
18) Shukla, Sandeep Kumar, and Manindra Agrawal. 2020. Cyber Security in India: Education, Research and Training. Springer Nature.
19) Stratton, Robert J. 2009. "Internet Security Threat Landscape." Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW '09. https://doi.org/10.1145/1558607.1558616.
20) Ullah, Rahmat. 2017. "Cyber Attack As A National Security Threat: South Asian Perspective." JOURNAL OF SOCIAL, HUMANITIES AND ADMINISTRATIVE SCIENCES. https://doi.org/10.31589/joshas.20.

PLAGARISM:



Page 1

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	992	Date	November 29, 2021
Characters	7125	Excluded URL	

5%	95%	2	40
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

ABSTRACT
Cybersecurity has come a complex and fast- moving security challenge in the age of Information Communication and Technology (ICT). As the dependence on ICT is heightening across the globe, cyberthreats appear likely to access every niche and corner of public husbandry and structure; indeed, the growing dependence on computers and Internet-grounded networking has been accompanied by increased cyberattack incidents around the world, targeting individualities, businesses, and governments. Meanwhile, ICT is decreasingly being seen by some governments as both a strategic asset to be exploited for the purposes of public security and as a battleground where strategic conflicts can be fought. This paper examines the supremacy of cybersecurity in the contemporary security debate, heightening the analysis by looking at the sphere of cybersecurity from the perspective of India.
KEYWORDS
Cyber security, Cyber Space, Terrorism, Human Rights, National trouble.
Preface
The conception of security is a core conception in the study of transnational relations. Traditionally, and until fairly lately, security analysis concentrated on state security, viewing it as a function of the situations of pitfalls which states face from other countries, as well as the manner and effectiveness of state responses to similar pitfalls. Still, after the end of the Cold War, scholars shifted focus from the state-centric notion of security, enlarging the conception to include the protection of the existent. (" Cyber Security Objects" 2012) At roughly the same time, the nature of pitfalls changed from external aggression tointra-state conflicts arising due to civil wars, environmental declination, profitable privation, and mortal rights violation. It's in this environment that public security came to include within its dimension other issues of security piecemeal from territorial protection, similar as poverty, artificial competitiveness, educational heads, environmental hazards, medicine and mortal trafficking, and resource dearths (Lobato,n.d.). Eventually, the recent Information, Communication and Technology (ICT) revolution — including the Internet, dispatch, social websites, and satellite dispatches — has revolutionised every aspect of mortal life, posing new challenges to public security. Indeed, in the digital age, the arena of public security is brazened with preliminarily strange pitfalls aimed at destroying a state's technology structure. It's an egregious banality that, in the globalized world, the Internet and ICTs are essential for profitable and social development, forming a vital digital structure upon which societies, husbandry, and governments calculate to perform their essential functions. The fairly open nature of the Internet guarantees that it is, on multitudinous situations, an unsafe terrain. (Lobato,n.d.; Shinde 2021) As similar, cybersecurity has come to encompass a wide range of issues similar as critical structure protection, cyberterrorism, cyberthreats, sequestration issues, cybercrime, andcyberwarfare.In the alternate decade of the twenty-first century, cyberthreats are evolving and adding at a fast pace. They're still initiated by felonious actors but also come from new sources, similar as foreign countries and political groups, and may have provocations other than plutocrat making. These ultimate may include some types of " hacktivism" in the name of a political cause, political destabilisation, cyberespionage, sabotage (e.g., Stuxnet), and indeed military operations (Lobato,n.d.; Shinde 2021; Graham, Olson, and Howard 2016). The complication of cybercriminals, the emergence of cyberespionage, as well as the well-publicised conditioning of hacker groups have combined to produce the print that cyberattacks are getting more systematized and that the degree of complication has increased significantly, showing clear signs of professionalisation. (Lobato,n.d.; Shinde 2021; Graham, Olson, and Howard 2016; Shukla and Agrawal 2020)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252

. Ideal

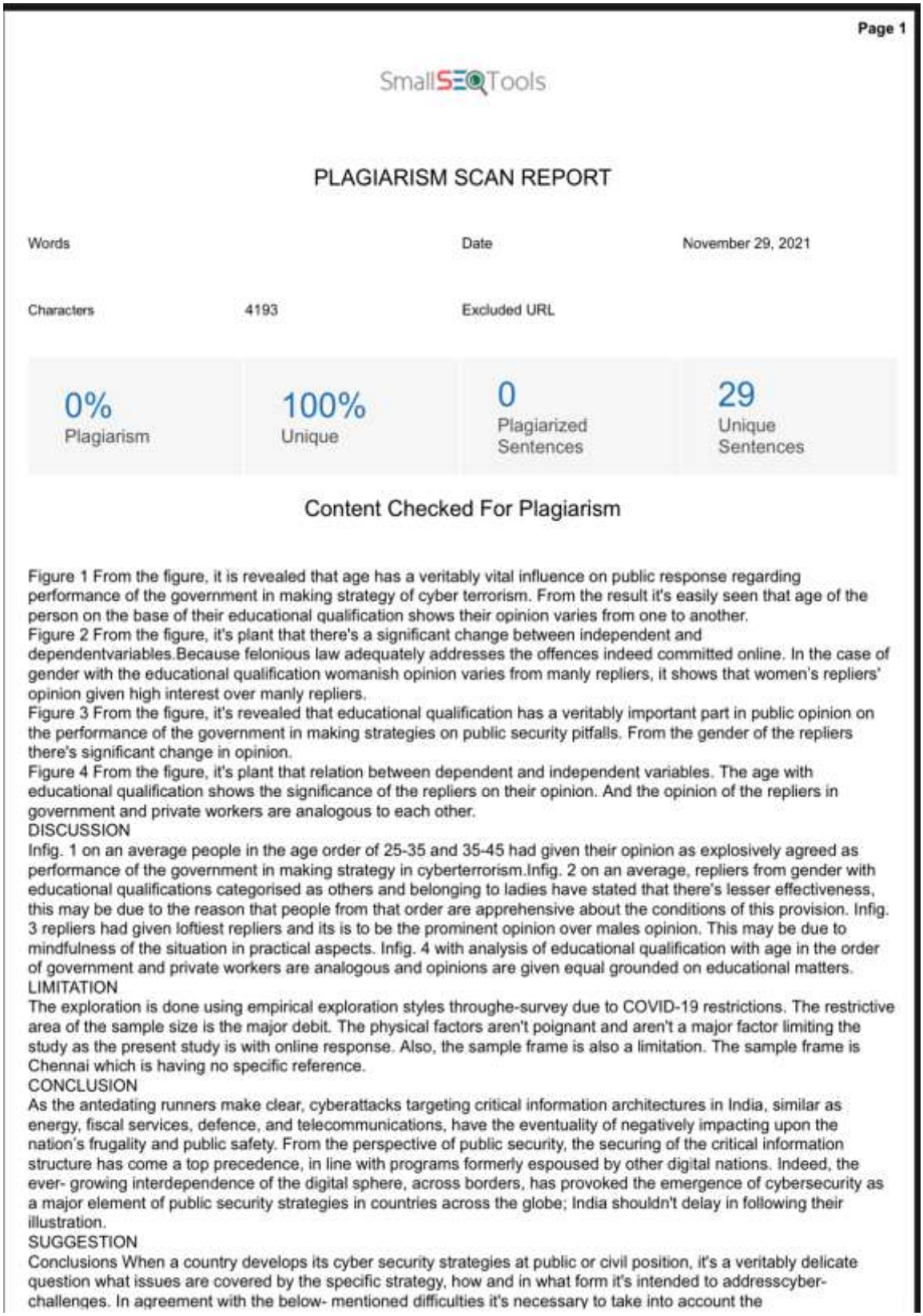
To make a secure and flexible cyberspace for citizens, businesses and Government.
To produce an assurance frame for design of security programs and for creation and enabling conduct for compliance to global security norms and stylish practices by way of conformity assessment.
To strengthen the Regulatory frame for icing a Secure Cyberspace ecosystem.
To help and respond to cyber pitfalls, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structure.

REVIEW OF LITERATURE

Network outages, computer contagions, data conceded by hackers, and other incidents affect our lives in ways that range from worrisome to life- hanging, as utmost government and fiscal institutions, military groups, pots, hospitals, and other businesses store and process an abundant deal of nonpublic information on computers. (Ambika, Ambika, and Senthilvel 2020) Therefore, with the adding volume and complication of cyberattacks, there's an increased need to cover particular information and sensitive business as well as to guard publicsecurity.Accordingly, the term " cybersecurity" refers to the collection of tools, programs, guidelines, training, conduct, security generalities and safeguards, threat operation approaches, assurance, and technologies that can be used to secure and cover the cyber terrain as well as organisation and stoner means (Ambika, Ambika, and Senthilvel 2020; " Cyber Victimization of Women and Cyber Laws in India,"n.d.). In addition, cybersecurity aims to secure information technology and focuses on guarding computer programs, networks, and data, along with precluding access to information by unauthorised druggies as well as precluding unintended change or intended/ unintended destruction (Ambika, Ambika, and Senthilvel 2020; " Cyber Victimization of Women and Cyber Laws in India,"n.d.; Gupta and Rao 2007). Likewise, cybersecurity plays a vital part in the ongoing development of information technology and Internet services. In the process, state security and countries' profitable well- being have come decreasingly reliant upon the successful protection of critical information architectures. Accordingly, in numerous countries, making the Internet as safe as possible is now integral to the development of government policy as well as new services. The rest of this composition examines the extent to which India has, to date, successfully dealt with this emergent challenge. In the Indian environment, the issue of cybersecurity has entered fairly little attention from policymakers, to the extent that the government has been unfit to attack the country's growing requirements for a robust cybersecurity outfit (Dasgupta 2009). In short, India lacks effective descent and protective cybersecurity capabilities, aggravated by the lack of access to mechanisms vital to defying sophisticated malware like Stuxnet, Flame, and Black tones. Also, cybersecurity systems and enterprise in India are far smaller in number as compared

Sources	Similarity
Cybersecurity in India: An Evolving Concern for National ... by SD Parmar · Cited by 1 — Cybersecurity has become a complex and fast-moving security challenge in the age of. Information Communication and Technology (ICT). https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf	34%

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 753-762 www.ijaem.net ISSN: 2395-5252



SmallSEOTools

PLAGIARISM SCAN REPORT

Words		Date	November 29, 2021
Characters	4193	Excluded URL	

0%	100%	0	29
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

Figure 1 From the figure, it is revealed that age has a veritably vital influence on public response regarding performance of the government in making strategy of cyber terrorism. From the result it's easily seen that age of the person on the base of their educational qualification shows their opinion varies from one to another.
Figure 2 From the figure, it's plant that there's a significant change between independent and dependentvariables.Because felonious law adequately addresses the offences indeed committed online. In the case of gender with the educational qualification womanish opinion varies from manly repliers, it shows that women's repliers' opinion given high interest over manly repliers.
Figure 3 From the figure, it's revealed that educational qualification has a veritably important part in public opinion on the performance of the government in making strategies on public security pitfalls. From the gender of the repliers there's significant change in opinion.
Figure 4 From the figure, it's plant that relation between dependent and independent variables. The age with educational qualification shows the significance of the repliers on their opinion. And the opinion of the repliers in government and private workers are analogous to each other.
DISCUSSION
Infig. 1 on an average people in the age order of 25-35 and 35-45 had given their opinion as explosively agreed as performance of the government in making strategy in cyberterrorism.Infig. 2 on an average, repliers from gender with educational qualifications categorised as others and belonging to ladies have stated that there's lesser effectiveness, this may be due to the reason that people from that order are apprehensive about the conditions of this provision. Infig. 3 repliers had given loftiest repliers and its is to be the prominent opinion over males opinion. This may be due to mindfulness of the situation in practical aspects. Infig. 4 with analysis of educational qualification with age in the order of government and private workers are analogous and opinions are given equal grounded on educational matters.
LIMITATION
The exploration is done using empirical exploration styles throughe-survey due to COVID-19 restrictions. The restrictive area of the sample size is the major debit. The physical factors aren't poignant and aren't a major factor limiting the study as the present study is with online response. Also, the sample frame is also a limitation. The sample frame is Chennai which is having no specific reference.
CONCLUSION
As the antedating runners make clear, cyberattacks targeting critical information architectures in India, similar as energy, fiscal services, defence, and telecommunications, have the eventuality of negatively impacting upon the nation's frugality and public safety. From the perspective of public security, the securing of the critical information structure has come a top precedence, in line with programs formerly espoused by other digital nations. Indeed, the ever- growing interdependence of the digital sphere, across borders, has provoked the emergence of cybersecurity as a major element of public security strategies in countries across the globe; India shouldn't delay in following their illustration.
SUGGESTION
Conclusions When a country develops its cyber security strategies at public or civil position, it's a veritably delicate question what issues are covered by the specific strategy, how and in what form it's intended to addresscyber-challenges. In agreement with the below- mentioned difficulties it's necessary to take into account the