Available online @ www.iaraindia.com
RESEARCH EXPLORER-A Blind Review & Refereed Quarterly International Journal
ISSN: 2250-1940 (P) 2349-1647 (O)
Impact Factor: 3.655(CIF), 2.78(IRJIF), 2.77(NAAS)
Volume XIII, Issue 43
July- 2024
Formally UGC Approved Journal (63185), © Author

CRITICAL ANALYSIS OF CYBER CRIME – THREAT TO NATIONAL SECURITY

SANJAY & RAKESH. IR
B.COM.LL.B (HONS)
School of Excellence in Law
Tamilnadu Dr Ambedkar law University, Chennai

Abstract

In the modern world of Information Communication and Technology (ICT), cybersecurity has developed into a challenging and quickly evolving security issue. Cyberthreats seem likely to target every aspect of national economies and infrastructure as the world's reliance on ICT grows. This paper delves into a critical analysis of cybercrime, its evolving landscape, and its impact on national security and emphasizes the urgent need for proactive measures to secure cyberspace and safeguard national security.

Keyword: Cyber-crime, Cyber security, National Security, IT.

Introduction

In today's increasingly digital world, Cybersecurity has become a serious concern for countries and organizations worldwide as reliance on technology continues to grow. India is not an exception. India's national security is greatly concerned about cyber security. The national security of India, as well as the welfare of its people, enterprises, and other interests, is seriously threatened by these challenges. In fact, an increase in cyberattack incidents targeting individuals, corporations, and governments has coincided with a growing global reliance on computers and Internet-based networking. It is mostly a web-based dispute involving a politically motivated cyber attacks on data and data infrastructure. Among many other things, cyber attacks have the ability to take down official websites and networks, interfere with or cease important functions steal or change classified material, and disrupt financial systems.

The implications of cyberspace crime for national security derive from the way technology is used by hostile elements. This paper suggests a policy-directed analysis of the definition of

cybercrime and its impact on the country's security. It has a description of collaboration between organized crime, criminals, and adversarial groups, It talks about the business of cyber reconnaissance and cyber assault capabilities, enabled by constantly advancing technologies and the expansion of the illegal market for IT services. At this point, cybercrime is hardly noteworthy outside of the domains of law enforcement and IT risk management.

Methodology

The doctrinal research approach is used in this paper. Secondary and tertiary statistics from sources like books, periodicals, essays, e-sources, newspapers, and other sources are used. Numerous magazines, articles, newspapers, journals, e-books, specific legislation acts, conventions, policies, regulations and schemes were referenced.

Objective of the paper

The overall objective of a research paper on cybercrime threats to national security would be to analyze the evolving landscape of cybercrime and its potential to compromise a nation's critical infrastructure, sensitive data, and overall stability. Here are some specific objectives that a research paper on this topic could address:

1. To identify and categorize the different types of cybercrime that pose a threat to national security. This could include cyber espionage, hacking of critical infrastructure, disinformation campaigns, and online extremism.
2. To assess the potential impact of cyberattacks on national security.
3. To evaluate the effectiveness of existing cyber security measures in mitigating cybercrime threats.
4. To identify the strengths and weaknesses of current cyber security policies, technologies, and international cooperation efforts.
5. To develop recommendations for improving cyber security preparedness and resilience.
6. To raise awareness about the growing threat of cybercrime to national security.

By addressing these objectives, a research paper is to help the policymakers and stakeholders in developing more effective strategies for protecting critical infrastructure, sensitive data, and national security from cyber attacks.

Cyber crime

The term "cyber crime" refers to a wide range of illegal activities, from electronic cracking to denial-of-service attacks, in which computers or computer networks are employed as a tool, a target, or a location. In terms of national security, cybercrime can include information warfare, classic espionage, and activism, along with its actions. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other’s benefit since decades. This gave birth to “Cyber Crime”. Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet. Cybercrime is often referred to as e-crime, high-tech crime, information age crime, computer-related crimes, etc. With more than 560 million internet users, India is the

second-largest online market in the world, behind China. People now depend on it for everything because of technology. The Internet is a "double-edged sword".

Cyber laws in India

There are a lot of disturbing incidents occurring in online these days. As the Internet is anonymous, it is possible for people to engage in a wide range of illegal actions with safety. As a result, wise people have been abusing this feature of the Internet brutally to further illegal activity in cyberspace. That's why India needs cyber laws.

1. The Information Technology Act, 2000
2. The Information Technology (Amendment) Act, 2008
3. Information Technology Rules, 2011
4. Indian SPDI Rules,2011 for Reasonable Security Practices
5. National Cyber Security Policy, 2013
6. National Cyber security Strategy 2020
7. Reserve Bank of India Act 2018
8. The Digital Personal Data Protection Act of 2023 (DPDP)

Additional legislation pertaining to cyber security includes Indian Penal Code 1860 (IPC), which penalizes offenses like defamation, cheating, criminal intimation, and obscenity performed online. The Companies Management and Administration Rules 2014, often known as the CAM rules, were established by the Companies Act of 2013 and mandate that businesses make sure their electronic records and security systems are protected from fraud and illegal access.

Where cyber do threats come's from

Cyber threats to national security encompass harmful actions in the digital domain that pose risks to a country's infrastructure, sensitive data, and overall stability. These dangers span cyber espionage, assaults on critical infrastructure, and the dissemination of disinformation. The potential outcomes extend from economic harm to the jeopardizing of military capabilities, underscoring the vital importance of robust cybersecurity measures in protecting national interests. Cyber threats come from numerous actors, including:

1. **Enemy Nations-States:**

National cyber warfare programs provide emerging cyber threats ranging from propaganda, website defacement, espionage, and disruption of key infrastructure to loss of life. There are more complex and present more advanced threats. Their growing powers have the potential to seriously and permanently harm the national security of numerous nations, including the US. Because they can use technology and tools to efficiently target even the most difficult targets, such as classified networks and vital infrastructures like gas control valves and electricity grids, hostile nation-states represent the greatest risk.

2. **Terrorist Organizations:**

Cyber attacks are a growing tool used by terrorist organizations to harm national interests. Compared to nation-states, they are less skilled at cyber attacks and are less likely to use cyberspace. Cyber terrorism, the use of digital tools and attacks for political or ideological motives, poses a significant and evolving threat to national security. Its potential to disrupt critical infrastructure, sow fear and discord, and undermine democratic processes makes it

a pressing concern for governments across the globe.

3. **Corporate Crime Organizations:** Organizations involved in organized crime and corporate spying provide a threat because they might carry out industrial espionage to steal trade secrets or substantial amounts of money. These parties typically have an interest to steal trade secrets, assaulting competitors' critical infrastructure, or getting access to and using it as take advantage of through blackmail. **Cybercrime groups t**hat target businesses and individuals for financial gain, often through malware, phishing scams, and ransom ware attacks.

4. **Hacktivists:**

Hacktivists work on a variety of political causes and objectives. Instead than causing harm to infrastructure or interrupting services, the majority of hacktivist organizations are more interested in distributing misinformation. Rather of trying to do as much harm as possible to an institution, their objective is to forward their political agenda. Motivated by political or social causes, hacktivists often target government websites and critical infrastructure to disrupt operations and raise awareness of their issues**.**

5. **Disgruntled Insiders:**

Insider dissatisfaction is a frequent cause of cybercrime. Since insiders may be permitted to view the data, they sometimes don't require much technical skills to reveal sensitive material. Employees or contractors with authorized access to systems can pose a significant threat if they become malicious or are compromised by attackers. Insider threats can be difficult to detect and prevent, as they have insider knowledge of systems and vulnerabilities.

Major Cyber crime which threaten National security of India

India, a rising digital powerhouse, faces a major cybercrimes that threaten its national security**.** With initiatives like Made in India and Digital India boosting the country's economy, India is quickly achieving its digital goals. However, its reliance on computer systems and networks, cyber security becomes a problem. India is one of the most cyber attacked nations; therefore securing vital resources depends on its cyber security resiliency. These digital onslaughts infiltrate critical infrastructure, steal sensitive data, and sow discord, potentially crippling the nation's stability and well-being. The digital battleground presents multifaceted threats to India's national security, fueled by diverse cybercrimes.

1. **Espionage and Data Breaches:** Malicious actors target government networks, critical infrastructure, and private businesses to steal sensitive data. Secrets that are essential to national security may be revealed through espionage, the covert act of taking confidential information. Cybercriminals or foreign intelligence services may attack defense contractors, government networks, or even seemingly innocent private businesses that store critical data.

Cyber attacks on Critical Infrastructure:

Power grids, transportation systems, and communication networks are vulnerable to cyber attacks. Sensitive information essential to national security is

stored in government databases, financial institutions, and communication networks. Cyberattacks may reveal sensitive information, interfere with financial transactions, and reduce public confidence in major entities. India's vital infrastructure is increasingly being the target of cyber attacks. The Kudankulum Nuclear Power Plant (KKNPP) experienced a cyber attack in 2019. An attack on the Mumbai Power Grid in 2020 resulted in a significant power outage, stopped trains in their tracks, and disrupted business activities.

2. Disinformation and Propaganda:

Imagine a network of fake information and faked films spreading around the internet to sow discord, distrust, and panic. Disinformation and propaganda campaigns weaponize information, aiming to destabilize communities, weaken national unity, and even trigger real-world violence. These digital wildfires pose a serious danger to national security because they may spread dissatisfaction throughout the country and decrease public faith in government institutions.

3. **Cyber terrorism:**

Terrorist groups may utilize cyber attacks to spread fear, disrupt critical infrastructure, and gain financial resources. There is both domestic and foreign terrorism existing in India when it comes to cyber terrorism. Cyberspace is used by corporations, government agencies, and military forces to store and handle large amounts of sensitive data. It helps the cyber terrorist in threatening national security. Terrorists primarily target India's administrative, economic, and security systems using cyber terrorism. India is attempting to stop this sophisticated form of terrorism using a variety of strategies.

4. Financial Cybercrime:

Cyberspace is not only a digital playground in today's interconnected globe, but also a battlefield for national security and economic stability. Financial cybercrime is a threat to India's financial sector and a long-term damage to the country's well-being. Budgets for national defense, public welfare, and stability as a whole may all be impacted as a result. India is able to protect its national security from the growing threat of financial cybercrime by implementing a various steps and international collaboration.

Reports on cyber-crime in India

Cybercrime is a rapidly growing threat in India, posing significant challenges to individuals, businesses, and national security. According to the National Crime Records Bureau (NCRB), cybercrimes in India increased by 24% between 2021 and 2022. Other crime categories also showed an increase, including economic offenses (11%), crimes against older persons (9%), and crimes against women (4%).

In 2022, the mean financial impact of a cyber-breach was recorded at $4.35 million. As per the "Crime in India" report, there were 65,893 incidents of cybercrime reported, which is a 24.4% rise from the 52,974 cases in 2021. "Under this category, the crime rate (per lakh people) grew from 3.9 in 2021 to 4.8 in 2022. According to the report, ransom accounted for 5.5% of cybercrime cases in 2022 (3,648 out of 65,893 cases), followed by sexual exploitation at 5.2% (3,434

instances) and fraud at 64.8% (42,710 out of 65,893 cases).

In the first half of 2023, approximately 12 lakh (1.2 million) cyber security events were reported to the Indian Computer Emergency Response Team (CERT-In), a 27% increase over the same time in 2022. According to a NortonLifeLock survey showed that 61% of Indian internet users reported having witnessed cybercrime in 2023. Financial fraud is the type of cybercrime that occurs most frequently in India. Between 2020 and 2023, this accounted for 75% of cybercrimes in India, with a peak of over 77% of crimes committed in that time frame.

Government role to protect national security

Protecting India's sovereignty, integrity, and security as well as its people from software that was stealing and surreptitiously transmitting users' data in an unauthorised manner to servers outside India were the stated aims of the restrictions. The Citizen Financial Cyber Frauds reporting and Management System **(**CFCFRMS**)** have over 10.10 lakh financial fraud instances recorded between January 1, 2023, and November 30, 2023. More than 4 lakh occurrences have resulted in savings of over Rs. 1000 crore since the CFCFRMS's launch on April 1, 2021. According to the research, India experienced over 400 million cyber threats across around 8.5 million devices in 2023, averaging 761 detections per minute. Bengaluru (14%) and Surat (15%) reported the greatest number of detections. According to a report released by the Data Security Council of India (DSCI) in partnership with enterprise cybersecurity solutions provider Seqrite, there were 49 million behavior-based detections, or 12.5% of the total detections.

The Indian government banned 59 mobile apps in 2020 because they were a threat to the country's defense, sovereignty, integrity, and public order. Under section 69A of the IT Act, 2000, the Ministry of Electronics and Information Technology (MeitY) blocked a total of 581 applications, comprising 174 applications related to betting and gambling, 87 applications for loan lending, and other applications, including gaming applications such as PUBG, GArena Free Fire, etc.

Steps taken by the government

India plans to tackle the rising issues of cyber security by enacting new privacy and encryption laws. In order to improve cyberspace security, it could potentially change the current legal framework. In order to address cyber security concerns, India established organizations and published the National Cyber Policy in 2013. India has recently started a number of cyber security programs to protect cyberspace and provide digital empowerment to its people. India named its first Chief Information Security Officer (CISO) in response to growing cyber threats. The appointment indicates India's determination to protect itself from cyberattacks. It will assist India in creating the vision and guidelines needed to combat cybercrime and improve cybersecurity management. To address cyber security, the government has implemented a number of legislative, technological, and administrative policy

measures. Indian Cyber Crime Coordination Centre (I4C): This center coordinates efforts to tackle all types of cyber-crimes across the country.

India's Cybersecurity Regulating Bodies:

1. Computer Emergency Response Team (CERT-In)
2. National Critical Information Infrastructure Protection Center (NCIIPC)
3. Cyber Regulations Appellate Tribunal (CRAT)
4. Securities and Exchange Board (SEBI) of India
5. Insurance Regulatory and Development Authority (IRDAI)
6. Telecom Regulatory Authority of India (TRAI) & Development of Telecommunications (DoT)

Recommendation

1. One of the main problems with India's regulations in the cyber security landscape is that the government still prosecutes under un-clarified or outdated statutes, which can hinder progress and the implementation of adequate cyber laws and regulations. It is challenging for organizations to determine the appropriate policies and recommendations for data privacy and cybersecurity from vague rules and mixed legislative approaches.
2. India has to enact more comprehensive and educational cyber security laws, as well as clarified rules and reforms to develop a better cyber security framework and data protection legislation, in order to maintain internationally recognized cybersecurity standards.
3. Create proper awareness to the public about the security issues in cyberspace and ask them to strengthen their cyberspace with security features such as strong antivirus software, use of the official version of the software, avoidance of popup messages and websites, proper updating of password etc.
4. Establish comprehensive legal and regulatory frameworks, such as stringent laws against cybercrime with definite fines, efficient data protection guidelines, and specific rules for intermediary accountability.
5. Funding for cyber security education and training needs to be increased in order to produce a workforce with the necessary skills to protect against cyber attacks.

Conclusion

Cyber security is a national imperative as well as a technical challenge. To maintain economic progress, preserve national security, and protect the welfare of its population, India must acknowledge the seriousness of cyber threats and proactively strengthen its digital defences. Through the implementation of a clear and proactive strategy, India can effectively negotiate the complex landscape of cyberspace and assure digital future. To become a digital powerhouse, India must take aggressive steps to strengthen its cyber security defenses and address cyber-attack concerns that threaten national interests. This includes investing in cyber security technologies, educating the public and companies on safe online practices, and setting in place strong security measures to safeguard key infrastructure.

In the case of a cybercrime, the government must also collaborate closely with corporations and international organizations. By doing so, India can safeguard its residents, businesses, and national interests security in the age of technology.

References

1. Pujari, A. (2016). Cyber Terrorism. World Wide Weponisation! TN Police Sesquicentennial Anniversary Souvenir.
2. Taneja, K. (2019, November 21). God‘s own Khilafat? Why Kerala is a hotspot for ISIS in India. ThePrint. https://theprint.in/pageturner/excerpt/god-own-khilafat-why-kerala-is-isis-hotspot-in-india/320945
3. Khetarpal, S. (2018). Data theft increased by 783% in India in 2017, says study. Business Today.https://www.businesstoday.in/technology/news/data-thefts-increased-783-percent-india-2017-gemalto-breach-level-index-study/story/277905.html
4. Chopra, R. (2019). In India, WhatsApp is a weapon of antisocial hatred. The Conversation.http://theconversation.com/in-india-whatsapp-is-a-weapon-of-antisocial-hatred-115673
5. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx
6. https://www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/
7. https://pib.gov.in/PressReleasePage.aspx?PRID=1845321
8. https://nsg.gov.in/nbdc/role-and-tasks
9. https://aag-it.com/the-latest-cyber-crime-statistics/
10. https://www.indusface.com/blog/digital-india-cybersecurity/
11. https://www.nist.gov/cyberframework
12. https://initiatives.weforum.org/global-cyber-outlook/home