INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

NATIONAL SECURITY THREAT IN CYBERSPACE

AUTHORED BY - ANANT KUMAR[1]

ABSTRACT:

The main aim of this paper is to provides information on recent trends of cyber threats and methods and raises concern about some dangerous cyber-attacks instances which has impacted the infrastructure and economic growth of the nation. These attacks directly and indirectly disrupted the essential services and endanger the public safety andnational security. Currently, people are not so much aware about the kinetic ramificationof cyber-attacks, but this paper analyses the unthinkable kinetic consequences of cyber-attacks and highlight the impact on human life. It also investigates the financial losses caused by cyber-attacks, focusing the flow of cyber-attacks money and analyses economic impact on individuals and nations.

Furthermore, the research examines the real-world application of the initiatives undertaken by India in its cybersecurity in the current scenario. The paper also exploresdifferent countries strategies for national security and their importance of proactive approaches in safeguarding against cyber threats.

KEYWORDS

National security, cyberspace, cyber-attacks, digital world

INTRODUCTION

Cyberspace means a virtual environment used by people to communicate over networks ofthe computer. In other words, it includes a web of computers and internet communication network which interconnect the world. In today's increasingly digital world, the use of internet cyberspace has grown at a global level where everybody is connected to each other.Many people and companies have used the cyberspace to grow their industries globally.[2]

[1] Student, BB. A LL. B-3rd Year, Bharati Vidyapeeth (Deemed to be University), New Law College, Pune
[2] Kathan Patel and Dhaval Chudasama, National Security Threat in Cyberspace: Available at Law journal (Volume 4, Issue 1, 2021). Also available at (PDF) National Security Threats in Cyberspace (researchgate.net)

ISSN: 2582-6433

This cyberspace is not only limited to the individual and companies, but the government organizations and sub-national groups are also used for functioning of institutions and for the development of the country. Moreover, it brings various security threat, where state sponsored hackers and terrorist groups uses cyberspace for attacking to governmentorganizations or an institution from which they try to steal sensitive information and intelligence services, and this pose direct attack to strategic, economic, and national interests of country. Safeguarding our country's interests and integrity is a part of national security. In this modern era, warfare has evolved beyond conventional arenas such as land,seas, air, and space. A significant threat has emerged as cyberspace. As the 21st century unfolds, the prospect of nations turning to cyberwar in times of conflict is increasing. Recognizing this, it is crucial for the government to fulfil its fundamental responsibility ofensuring national security, protecting citizens, the economy, and institutions.

CYBER THREATS AND METHODS

On any given day, we hear news of hacking incidents and damage to systems, typically assuming that it involves the breach of a company's security, with hackers attempting to steal information such as names, email addresses, and personal details. However, the realityof cyber threats extends far beyond these common scenarios. In today's world, a multitudeof methods aim to disrupt critical infrastructure, ranging from nuclear power plants to the stock market. Disruptions in pivotal sectors like energy, finance, or space exploration can have profound and cascading effects on a country's overall functioning. A recent example in India is the Indian Space Research Organization (ISRO), which faced multiple cyber- attacks following the successful completion of Chandrayaan-3. It highlights that cyber threats encompass various methods and pose significant risks across different sectors. Certainly, here are some main types of national security threats in cyberspace.[3]

Method 1- RANSOMWARE ATTACKS

Ransomware attacks involve malicious software that encrypts a victim's data, rendering it inaccessible. The attacker then demands a ransom in exchange for restoring access. This can cripple critical systems, leading to operational and financial disruptions. This attack isalso called as digital kidnapping, where a dangerous software threatens to leak your privatephotos or any data

[3] Abhi and Niyu.[Abhi and Niyu](2023,9jun).Why India needs cybersecurity. YouTube .https://youtu.be/pWpqj1GlDJI?si=UhsrrXNkjOBqFzl1

ISSN: 2582-6433

of your system.

AIIMS DELHI CYBER ATTACKS

On November 23, 2022, a cyber-attack was detected in AIIMS' internal systems, leading to a significant impact on the hospital's digital patient management system. In a confirmed statement, AIIMS recognized the difficulty in restoring data, attributing it to the extensive server infrastructure that handles 15 lakh outpatient and 80,000 inpatient cases each year. The compromised data includes highly sensitive information such as names, age, gender, addresses, phone numbers, and medical histories of all patients. In reports, Delhi Police refuted claims suggesting that hackers were demanded a Rs. 200 crore crypto ransom to release their hold on the system.[4]

Method 2- SOCIAL ENGINEERING ATTACKS

Social engineering is a manipulative strategy that exploits human psychology to extract confidential information or induce individuals into compromising security. Common techniques include phishing, where deceptive emails or messages lure victims into revealing sensitive data, pretexting involves creating a fabricated scenario to extract information, and baiting entices individuals with something enticing, like a free download, to compromise security.[2]

- **USB DROP ATTACKS**

USB drop attacks are quite famous in America where in an organisation, hackers randomly leave pen drive or hard drives. The one who gets this device goes to become a good person. Thinks someone may have dropped it but who. He connects the computer to find out. When the victim connects the USB drive, their computer recognizes it as a keyboard. However, these drives are loaded with malicious code, granting hackers unauthorized access to the connected computer. A similar attack happened with the American military in 2008, when at their middle east base hackers got access to their confidential computers.[5]

Method 3-PHISHING

Phishing emerges as a trending cybersecurity concern for national security in the digital world,

[4] Bharat Sharma, What's Happening at AIIMS After Sensitive Ransomware Attack? (2 DEC 2022) available at Explained: What's Happening At AIIMS After Sensitive Ransomware Attack? (indiatimes.com)
[5] Bharat Sharma, What's Happening at AIIMS After Sensitive Ransomware Attack? (2 DEC 2022) available at Explained: What's Happening At AIIMS After Sensitive Ransomware Attack? (indiatimes.com)

ISSN: 2582-6433

employing deceptive methods to manipulate individuals and attain unauthorized entry to confidential information. This type of cybercrime commonly involves the use of deceitful emails, messages, or websites that looks legitimate, aiming to deceive individualsinto disclosing private data like login credentials, personal details, or financial information.[2]

- **YOUTUBE PHISHING ATTACK**

In this attack, Cybercriminals sent deceptive emails from same official email id of YouTube, falsely notifying users for changes to the platform's rules and policies. The mailclaims that the company is updating its monetization regulations. It mentions an 'official document' related to these changes and urges users to download it through a provided link.[6]

Method 4- DDoS (DISTRIBUTRED DENIAL-OF-SERVICE)

Denial-of-Service (DoS) attack affects a system, network, or website with excessive traffic,making it inaccessible to users. Distributed Denial-of-Service (DDoS) attacks compound this threat by leveraging multiple systems to intensify the assault. This is especially alarming for national security, as DDoS attacks can disrupt critical infrastructure, impede communication channels, and compromise essential services.

- **AIRPORTS CYBERATTACKS IN INDIA**

On April 8,a DDos attack targeted six prominent airports and healthcare institutions in India. The attack was executed by a hacktivist group called Anonymous Sudan, focusing on critical infrastructure, including airports in Delhi, Mumbai, Hyderabad, Goa, and Kochi.[8]

UNTHINKABLE CONSEQUENCES OF CYBER ATTACK

Over the past decade, the consequences of cyber threats have undergone significant changes. The term "cyberwar" didn't exist 30 years ago and now it is controversial. **The Armis State of Cyberwarfare and Trends Report: 2022-2023** report the evolving scenario, emphasizing how technology has impact in the life of people through cyber threats.[5]

The report stated that Artificial Intelligence (AI) and Machine Learning (ML) are increasingly pervasive in technology. These technologies play a crucial role in automatingthe identification

[6] Divyanshi sharma, Received an email about YouTube changing its policies? It might be a phishing attempt, do not fall for it. Available at Received an email about YouTube changing its policies? It might be a phishing attempt, do not fall for it - India Today

ISSN: 2582-6433

and response to cyber threats. However, the report notes that concern about the potential misuse of AI and ML for malicious purposes. And emphasizing the needfor enhanced rules and regulation. Further, it raises concern about the use of generative AItools, such as ChatGPT for creating malicious code.

The CTO and co-founder of Armis, Nadir Izrael, states in the report's foreword that analystsproject that threat actors would be able to weaponize operational technology (OT) environments by 2025 in order to harm or kill people. He notes that it is a part of a trend incyberwarfare that shifts the focus from espionage and reconnaissance to kinetic applicationwith practical ramifications.

While several of these kinetic cyberweapons have been detected in the world, none of themhave been used in a way that is fatal. For example,
In 2017, the Triton malware posed a significant risk by specifically targeting to disabled the Safety Instrumented System (SIS) controllers at a petrochemical plant in Saudi Arabia.If it was undetected, this cybersecurity breach had the potential to initiate a disastrous, plant-wide incident. The Triton episode underscores the susceptibility of critical infrastructure to sophisticated cyber threats, emphasizing the immediate need for robust cybersecurity measures to detect and mitigate such risks. This event highlights the critical importance of securing industrial control systems and the potential consequences when malicious actors successfully compromise the safety mechanisms integral to the functioning of vital facilities.

In February 2021, an unidentified hacker was attacking the operations technology (OT) system of a water treatment plant in Oldsmar, Florida. The cyberattack aimed to contaminate the water supply by manipulating the sodium hydroxide levels from 100 partsper million to a dangerous 11,100 parts per million. Fortunately, a vigilant operator detectedthe intrusion and promptly reversed the altered settings, preventing the infusion of hazardous levels of the chemical into the water. This incident underscores the critical importance of cybersecurity in safeguarding essential infrastructure and highlights the potential devastating consequences of cyber threats on public safety.[7]

[7] Tony Bradely, New Report Highlights Concerning Trends For Cyberwarfare available at FORBES, New Report Highlights Concerning Trends For Cyberwarfare (forbes.com)

ISSN: 2582-6433

FINANCIAL LOSSES FROM CYBER ATTACKS

If considered as a nation, cybercrime, expected to cause global damages amounting to $6 trillion USD in 2021, would rank as the world's third-largest economy, following the U.S.and China.

The **Cybersecurity Ventures report** anticipates an annual 15 percent growth in global cybercrime costs over the next five years, with projections reaching $10.5 trillion USD annually by 2025, a significant increase from $3 trillion USD in 2015. This marks a greatertransfer of economic wealth in history. The anticipated costs surpass the damages from natural disasters and will be more profitable than combined global trade profits of major illegal drugs. The estimation considers historical cybercrime data, recent growth trends, a substantial rise in state-sponsored and organized crime gang hacking, and an expected tenfold increase in the cyberattack surface by 2025 compared to the present. This Cybercrime expenses encompass various damages such as data damage and destruction, financial losses, diminished productivity, intellectual property theft, personal and financial data breaches, embezzlement, fraud, disruptions post-attack, forensic investigations, data and system restoration and deletion, and reputational harm.[8]

In 2021, Asia was most attacked region by cybercriminals, constituting one in four global attacks, with India ranking among the top three nations experiencing a high number of server access and ransomware attacks in the region, as per a recent report. Server access attacks (20%) and ransomware incidents (11%) topped the list of attacks on Asian organizations in 2021.[9]

According to a Microsoft study in 2022, 31% of Indians experienced financial losses due to cyber-attacks, affecting nearly 50 crore individuals who lost their hard-earned money. The above data is a cause for concern regarding India's growth and it directly impacting thegoal of reaching a $5 trillion GDP, as cyber-attacks pose a threat to economic stability.

WHERE ARE GOING THE CYBER ATTACK MONEY?

After considering the above information, a crucial question arises: Who benefits from the money acquired through cyber-attacks? While the immediate assumption may point to terrorists' organizations, but the reality goes beyond this simplistic view.

[8] Steve Morgan, Cyberwarfare in The C-Suite.(13 nov 2022 Available at Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)
[9] IANS, Cyber-attacks: India among top 3 most-affected nations in Asia in 2021 available at business standard(24 FEB 2022) Cyber attacks: India among top 3 most-affected nations in Asia in 2021 (business-standard.com)

ISSN: 2582-6433

Chainalysis, is an American research company, conducted a comprehensive tracking of hacked money, revealing shocking facts. That, 74% of the hacked funds transfer to Russia.

Presently, North Korea stands as one of the world's most dangerous countries, possessing nuclear weapons. The country faces numerous sanctions that restrict its ability to engage inregular trade for economic sustenance. As a result, North Korea turns to illegal activities means, including cybercrime. It was revealed in US senate that a significant portion of North Korea's missile program, about one-third, has been funded through proceeds from cyberattacks.

India, with its huge number of populations of internet users, has witnessed a remarkable digital transformation, with more than 52% of its population, equivalent to 759 million individuals, accessing the internet monthly in 2022. This surge in connectivity has make India into a rapidly expanding digital economy, where sectors such as healthcare, education, finance, retail, and agriculture increasingly rely on online platforms and services. Recognizing the imperative to secure its digital infrastructure and data, India hasimplemented a series of strategic initiatives to fortify its cybersecurity landscape. The policy is –

1. **National Cyber Security Policy (NCSP):** A comprehensive framework designed to establish a secure and resilient cyberspace environment. The main aim of NCSP is to encompass heightened cybersecurity awareness, securing critical information infrastructure, and promoting research and development in the field.
2. **National Cyber Coordination Centre (NCCC):** It serves as a pivotal hub in India's cybersecurity apparatus. Functioning as a centralized entity, the NCCC is dedicatedto monitoring and responding to cyber threats in real-time. It facilitates seamless information sharing and coordination among diverse government agencies, fostering a collaborative and proactive approach to cybersecurity.
3. **Indian Cyber Crime Coordination Centre (I4C):** The Indian Cyber Crime Coordination Centre (I4C) plays a crucial role in combating the escalating menace of cybercrime. It aims to strengthen law enforcement, address cyber threats, enhance digital forensics, and coordinate actions to combat cybercrime efficiently.
4. **National Critical Information Infrastructure Protection Centre (NCIIPC):** Addressing the protection of critical information infrastructure, the National Critical Information Infrastructure Protection Centre (NCIIPC) identifies and designates critical sectors. It formulates guidelines for their safeguarding, diligently working towards enhancing their cybersecurity resilience.

ISSN: 2582-6433

5. **Cyber Security Awareness Programs:** These campaigns and programs play a pivotal role in educating citizens, businesses, and government officials about best cybersecurity practices, fostering safe online behavior, and underscoring the critical importance of securing digital information.[10]

However, these above efforts remain inadequate as India faces a shortage of technical staff, insufficient cyber forensics facilities, a lack of cyber security standards, and challenges in coordinating among various stakeholders. Moreover, in October 2023, Resecurity, a US- based company, brought to the world's attention the presence of Indians' personal data on the dark web. The seller of the dataset was offering verifiable, sensitive information pertaining to 55% of the Indian population, roughly around 815 million (81.5 crore) citizens. This included personally identifiable information such as names, phone numbers,Aadhaar numbers, passport numbers, and addresses[11]. In the absence of the effectiveness of these initiatives, there arises a legitimate concern about relying on outdated policies. TheNational Cyber Security Policy, formulated in 2013, had played a pivotal role in guiding the government in cybersecurity practices. However, in the wake of rapid technological advancements, there is a immediate need to address these issues at the highest level and adopt a comprehensive approach.[3][2]

COUNTRIES STRETAGY TO SECURE CYBERSPACE

A nation's concerted effort to defend its interests, infrastructure, and digital environment from cyber threats is known as its cyberspace strategy. This framework comprises objectives, guidelines, and steps to enhance risk management, cybersecurity, and incident response. To safeguarding the essential infrastructure, protect citizen privacy, and foster international cooperation for a safe digital ecosystem, it makes use of legal, technological,educational, and diplomatic methods.

Various countries use various approaches to safeguard cyberspace, acknowledging its crucial significance for both public welfare and national security. As an example:

1. **United States (U.S.):** Public-private partnerships are a main component of the U.S.A approach for their cybersecurity. The cooperation between government and business

[10] IGNOU services, what are different initiatives taken by Indian government? Available at Define IT act and its amendment. What are the different initiatives taken by Government of India for protecting country's information assets? (ignouservice.in)
[11] India's Cybersecurity Challenge: Threats and Strategies (26 dec 2023) . available at India's Cybersecurity Challenge: Threats and Strategies (drishtiias.com)

ISSN: 2582-6433

sector encouraged by initiatives. i.e, the National Institute of Standards and Technology (NIST), which laid guidelines for critical infrastructure cybersecurity.

2. **Estonia**: Estonia, known for its leadership in e-governance, places a strong emphasis on cyber resilience, particularly after a significant cyber-attack in 2007. In response, the country work on its cybersecurity infrastructure, introducing advanced measures to enhance its defences. A noteworthy initiative included the establishment of the NATO Cooperative Cyber Defence Centre of Excellence. Thiscentre functions as a focal point for global cooperation, research, and training in cybersecurity, underscoring Estonia's dedication not only to fortifying its own security but also to contributing on an international scale to the advancement of cyber resilience and protection in the digital realm.
3. **Israel**: Renowned for its expertise in cybersecurity, Israel integrates military intelligence with private sector ingenuity. The elite intelligence unit, Unit 8200, functions as a talent reservoir for cybersecurity professionals, augmenting the nation's cyber capabilities.
4. **South Korea:** This nation prioritizing cybersecurity education, through initiatives like the Korean Internet Security Agency (KISA), focuses on cultivating a proficient workforce to combat emerging cyber threats.
5. **Singapore:** Singapore adopting a comprehensive approach that incorporates legislation such as the Cybersecurity Act and promotes collaboration via the CyberSecurity Agency (CSA). The city-state also commits to research and development in emerging technologies to fortify its cybersecurity landscape.

These above countries have made significant efforts to strengthen their cybersecurity and protect national interests in the digital environment. These measures not only safeguard thecountry but also foster a secure business environment, gaining trust from investors and entrepreneurs. The initiatives undertaken highlight their cyber resilience, showcasing theirability to prepare for, respond to, and recover from cyber threats. This not only promotes asecure digital landscape but also encourages economic activities by assuring businesses ofa safe and resilient cybersecurity infrastructure.

ISSN: 2582-6433

CONCLUSION AND RECOMMENDATION

In this paper, I have discussed some of the threats that can impact national security. While Cyberspace can be used as a platform for showcasing innovation and prosperity but its largeand loosely regulated digital infrastructure creates significant threats to nations, businesses, and individuals. It is crucial for governments to address potential vulnerabilities and recognize that cybersecurity is important for national security in today's world. Treating the digital infrastructure as a national asset is essential, and protective measures should beimplemented. With the constant growth of new technologies like artificial intelligence, therisk of cyber warfare should be taken as seriously as that of a nuclear missile. The increasing dependency on computers makes every nation vulnerable to cyber-attacks, emphasizing the need to make country cyber resilience. In today's world, the occurrence ofa cyber-attack is not a question of if but when, and being proactive is crucial to reducing its impact.