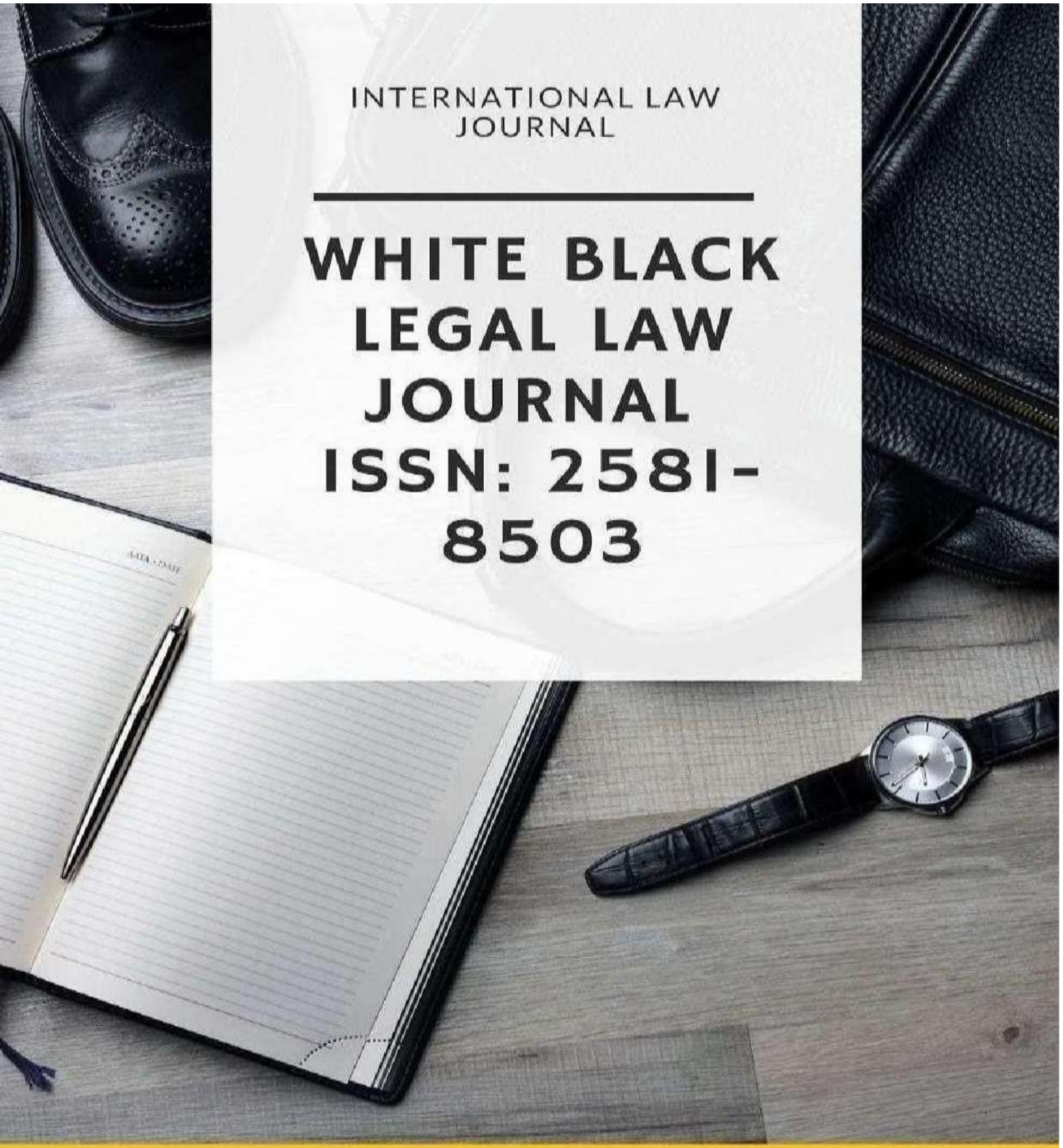

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

MAJOR CYBER ATTACK IN INDIA

AUTHORED BY - ABHISHEK KUMAR & PUSHPA SINGH

Abstract

The rapid growth of internet usage in India has brought many benefits, but it has also led to an increase in cybercrimes. These crimes are serious threats to people, businesses, and even national security, including harmful activities like malware attacks, hacking, and bot usage. As India becomes more dependent on digital systems, it has become a prime target for cybercriminals. The rising frequency and complexity of these threats can be seen in major incidents like the cyberattack on AIIMS Delhi, large personal data leaks on the dark web, and targeted attacks on Indian vaccine companies. These cybercrimes not only disrupt essential services but also cause financial losses, data theft, and sometimes political instability. Both the public and private sectors in India have been affected by cybercriminals, who exploit weak points through various techniques. In 2023, India saw 5.3 million hacked accounts, ranking fifth in the world for cyberattacks—a significant increase from previous years. Many of these attacks are carried out by organized crime groups and state-backed hackers driven by financial or political motives, often using the dark web to operate. Since cybercriminals can be anywhere, it's hard to track and catch them. To tackle these threats, the Indian government has introduced laws like the Information Technology Act of 2000, certain sections of the Indian Penal Code, and created the Indian Computer Emergency Response Team (CERT-In). These efforts provide a legal basis to pursue cybercriminals and secure important systems. The upcoming Data Protection Bill will also help protect citizens' privacy by controlling how personal data is collected, stored, and used.

Introduction

This era is computer, and mostly every young person uses the internet for doing his work. They use the internet for studying, banking, playing games, online employment, etc. This internet is intended to be used for good deeds and to simplify everyday tasks. A young person depends on the internet. Like technology is increasing every day, same-bed activity is increasing every day. They use it for phishing, illegal downloading, bank robbery, Credit card frauds, industrial espionage, kidnapping children via chat rooms, scams, child pornography, cyber terrorism, creation and or distribution of viruses, spam and so on.. It is dangerous to private and public persons. Many times it created problems for national. They use the hacking system of government agencies and theft of important information data.

The term "cybercrime" describes illicit actions directed towards or taking advantage of computers, computer networks, or related equipment. Even while money is the main driver behind most cybercriminals, there are other reasons why they commit cybercrimes, like creating harm, upsetting political systems, or harboring personal grudges. Data theft, fraud, and intentional system damage are just a few examples of these attacks. Cybercriminals frequently employ sophisticated techniques to break into networks and steal confidential data, while other cybercriminals concentrate on causing service interruptions or stealing money[1].

Cybercrime can be committed by one person, a group of people, or an organization. Some cybercriminals use highly specialized talents and sophisticated procedures, and they are a part of organized networks. However, inexperienced hackers also engage in cybercrime; they typically cause harm by taking advantage of easier weaknesses. Irrespective of the incentive or proficiency, cybercrime presents noteworthy hazards to international governments, corporations, and private citizens[2].

Cybercrime is distinct from all other forms of criminal activity in the community. The reason for this is that cybercrime knows no geographical bounds and its perpetrators are unknown. It has an impact on all parties involved, including the government, businesses, and residents. the incidence of cybercrime in India. He also goes over various strategies for combating cybercrime in India.

[1] Singh, Anamika, Cybercrime In India Challenges And Solutions, 2021 Page No. 1-20, Banaras Hindu University

[2] Ibid

In 2023, India had 5.3 million compromised accounts, ranking fifth among countries with the highest number of breaches. Globally, there were 299.8 million compromised accounts, with the United States leading the list, accounting for 32% of all breaches between January and December. In 2022, India was ranked seventh with 12.3 million compromised accounts. The United States, which had previously ranked third in 2022 with 31 million compromised online accounts—following China and Russia—rose to the top spot in 2023 with approximately 100 million compromised accounts, marking a threefold increase from the previous year[3].

Cybersecurity Ventures predicts that global cybercrime costs will increase by 15 percent annually over the next five years, reaching $10.5 trillion USD per year by 2025, up from $3 trillion USD in 2015. This marks the largest transfer of economic wealth in history, threatening innovation and investment, causing damage far exceeding that of natural disasters in a year, and becoming more profitable than the global trade of all major illegal drugs combined[4].

This cost estimate is based on past cybercrime data, recent year-over-year growth, a significant rise in cyberattacks sponsored by hostile nations and organized crime groups, and a cyberattack surface that will be vastly larger by 2025 than it is today. The deep web—an area of the internet that is intentionally hidden and used to obscure and facilitate criminal activities—is believed to be as much as 5,000 times larger than the surface web, growing at an unmeasurable rate. The dark web, a part of the deep web, is where cybercriminals trade malware, exploit kits, and cyberattack services, which they use to target victims, including businesses, governments, utilities, and essential service providers in the India.

MAJOR CYBER ATTACK

Cyberattacks targeting India have been on the rise, primarily driven by motives related to data privacy breaches, financial theft, espionage, and geopolitical tensions. Countries like China and Pakistan, and other countries are often accused of organizing these attacks to gain strategic advantages or disrupt critical infrastructure in India. While some of these cyberattacks have succeeded, India has managed to thwart many, showcasing improvements in cybersecurity resilience. Below are some notable incidents of cyberattacks in India:

[3] India Ranks Amongst The Top Five Most Breached Countries In 2023, Finds Analysis, The Hindu Bureau, February 26, 2024

[4] Steve Morgan, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Nov. 13, 2020

1. AIIMS Delhi Cyber Attack

In December 2022, the All India Institute of Medical Sciences (AIIMS) Delhi experienced a significant cyber attack reportedly originating from China and Hong Kong. The Delhi Police's Intelligence Fusion and Strategic Operations unit has reached out to the Central Bureau of Investigation (CBI) for information from Interpol regarding the IP addresses associated with email accounts linked to the attackers. An FIR for extortion and cyber terrorism has been filed by the Delhi Police's cyber cell based on AIIMS' complaint. While there have been claims of hackers demanding Rupees 200 crore for the decryption key, the police have refuted these allegations. The cyber attack disrupted various digital services at the hospital, including outpatient and inpatient management systems, smart laboratory functions, billing, report generation, and appointment scheduling[5].

2. ISRO warned of a possible cyberattack when Dtrack came calling[6]

North Korean hackers targeted the Indian Space Research Organisation (ISRO), but the attack did not affect the space agency. An ISRO official confirmed that they received an alert from the Computer Emergency Response Team, India (CERT-In). Yash Kadakia, the founder of Mumbai-based cybersecurity firm Security Brigade, revealed that he had evidence of malware-laden emails being sent to five government agencies, including ISRO, by suspected North Korean hackers. The alert was issued around the time of the Chandrayaan-2 mission. If the malware had been successfully installed, it could have hijacked the recipient's email identity, enabling the hackers to send emails to subordinates under the guise of the compromised identity.

3. Surge in cyber attacks on Indian vaccine makers

Between October 1 and November 25, 2020, there was a significant increase in cyber attacks on Indian vaccine makers and hospitals. According to the Cyber Peace Foundation, nearly 8 million attacks were recorded during this period on a network specifically set up to monitor threats in the healthcare sector in India. In October alone, there were 5,434,825 attacks, and by November, there had already been 1,643,169 attacks.

The Foundation also noted that many ransomware attacks targeted the healthcare sector during

[5] Aashish Aryan, Ettech, Aiims Cyber Attack Took Place Due To Improper Network Segmentation: Govt In Rs., The Economic Times, Feb 10, 2023

[6] ISRO Warned Of a Possible Cyberattack When Dtrack Came Calling, The Economic Times, Nov 08, 2019

the COVID-19 crisis, particularly starting from April 2020. The most common types of ransomware used in these attacks were 'NetWalker ransomware', 'PonyFinal ransomware', and 'Maze ransomware[7]'

4. Data Breach of 81.5 crore Indians: Aadhaar, Passport Details Leaked on Dark Web

A significant data breach has reportedly exposed the personal information of over 81.5 crore Indian citizens on the dark web. The compromised data includes Aadhaar numbers, passport information, names, phone numbers, and addresses, and is believed to have originated from the Indian Council of Medical Research's (ICMR) database. The breach, which was first reported by the US-based cybersecurity firm Resecurity, has prompted the Central Bureau of Investigation (CBI) to consider an investigation once ICMR files a formal complaint. Despite these reports, the Indian government has yet to officially confirm the breach[8].

The breach was uncovered by Resecurity's HUNTER (HUMINT) unit, which identified the stolen personally identifiable information (PII) being sold by a hacker known as 'pwn0001' on Breach Forums on October 9. The hacker provided proof of the breach by sharing spreadsheets containing Aadhaar data, which Resecurity verified against a government website. This verification confirmed the authenticity of the data, highlighting the severity and potential impact of the breach, which could be one of the largest in Indian history.

Additionally, another hacker named 'Lucius' claimed to have leaked an even larger 1.8 terabyte data set on August 30. This data reportedly includes Aadhaar IDs, Voter IDs, and driving license records, and may have originated from an internal Indian law enforcement organization. Some records were labeled "PREPAID," suggesting the possibility that the breach could have been sourced from a telecommunications company that collects personal information for prepaid SIM card verification.

5. DRDO Scientist Kurulkar Honey-Trapped by Pakistani Agent

Pradeep Kurulkar has been appointed as the Director at the Systems Engineering Laboratory of the Research & Development Establishment (Engineers) [R&DE(E)], which is a part of the

[7] Cybersecurity Firm Sophos Hit By Data Breach, Says 'Small Subset' Of Customers Affected, Et Cio. Com , Nov 27, 2020

[8] Data Breach Of 81.5 Crore Indians: Hacker Allegedly Leaks Aadhaar, Passport, Personal Details On Dark Web, Bt Business Today, Oct 31, 2023

Defense Research and Development Organization (DRDO). He played an important role in developing and designing several military engineering equipment and systems. As a lead designer and team leader, he contributed to projects like hyperbaric chambers, high-pressure pneumatic systems, mobile power supplies, and missile launchers for various programs such as AD, MRSAM, Nirbhay subsonic cruise missile system, Prahar, QRSAM, and XRSAM.

According to a chargesheet filed by the Anti-Terrorism Squad (ATS) of the Maharashtra police, DRDO scientist Pradeep Kurulkar was allegedly tricked by a Pakistani intelligence agent using the fake name 'Zara Dasgupta'. 'Zara Dasgupta' pretended to be a software engineer living in the UK and made contact with Kurulkar by sending explicit messages and videos. The chargesheet reveals that Kurulkar and 'Zara Dasgupta' communicated through WhatsApp, as well as voice and video calls.

The Pakistani agent attempted to obtain classified and sensitive information about various defense projects, including the Brahmos Launcher, Drone, Unmanned Combat Vehicle (UCV), Agni Missile Launcher, and Military Bridging System. Kurulkar, who was attracted to her, stored this classified information on his personal phone and allegedly shared it with 'Zara'.

6. First case of 'digital kidnapping' in Punjab

The first instance of 'digital kidnapping' in Punjab saw cybercriminals demanding ransom from a pharmaceutical company. On July 19, 2016, employees of Shri Dhanvantari Herbals, an Ayurvedic pharmaceutical company in Amritsar, Punjab, arrived at work as usual. However, when they turned on their computers, they were shocked to find that cybercriminals had taken control, locking them out of the system.

The company soon received a ransom demand from the criminals, who insisted on being paid in Bitcoins, a digital currency that is hard to trace. Despite attempts to negotiate through the provided email, the company couldn't reach an agreement with the criminals[9].

The Punjab Police’s Cyber Crime Cell is working hard to track down the criminals, but it's challenging since they may be operating from another country and are using strong encryption.

[9] First Case Of 'Digital Kidnapping' In Punjab, Cyber Criminals Seek Ransom From Pharma Company, India Today, Aug 24, 2016

The police have registered a case and started investigations, with plans to seek help from Interpol if necessary. They've also consulted with the I-T department, Mumbai Police, and private cyber experts. The police are advising the public to avoid visiting illegal websites, downloading unauthorized software, and clicking on suspicious ads.

7. The Freedom 251 smart Phone

Mohit Goel, the mastermind behind the Freedom 251 mobile phone scam, gained widespread attention across India for offering a smartphone at an unbelievably low price of just ₹251. Promoted as the world's cheapest smartphone, the phone quickly attracted millions of potential buyers. His company, Ringing Bells, aimed to sell 5 million units, but the website crashed on the first day due to overwhelming traffic, and only 30,000 units were booked, generating around Rupees 40 lakh[10].

As complaints began to pile up, many customers who pre-booked the phone never received it. Investigations revealed that the entire operation was fraudulent. Goel was arrested, and it was discovered that he was involved in criminal activities across several states. The Freedom 251 scam became a notorious case of failed promises and fraudulent business practices.

8. The Reserve Bank of India

The Reserve Bank of India (RBI) has expressed concern over the rise in cyber security breaches within the banking sector, with 248 successful data breaches reported between June 2018 and March 2022. Most breaches involved card details leakage and theft of business information, with public sector banks reporting 41 cases, private banks 205, and foreign banks two. The RBI has directed banks to enhance their IT risk governance framework, involving chief information security officers and board-level oversight to ensure compliance with security standards[11].

This caution comes after the RBI's Cyber Security and Information Technology Examination (CSITE), which is distinct from the regular annual risk assessment. The CSITE evaluates banks' disaster management, internet and mobile banking capabilities, and fraud detection efficiency, identifying weaknesses and issuing action points for improvement[12].

[10] Mohit Goel, Man Who Tried To Sell Freedom 251 Phone For Rs 251, Arrested In Dry Fruits Business Fraud, India Today, Aug 25, 2021

[11] Jocelyn Fernandes, Rbi Alerts Banks On Heightened Cyber Security Threats, Gives Action Plan To Address Vulnerabilities , Mint, 18 Mar 2024,

[12] Indian Banks Reported 248 Data Breaches In Last Four Years, Moneycontrol News, August 02, 2022

Further, the RBI's alert follows a report by the Data Security Council of India, highlighting that 25% of cyber attacks in the country stem from malicious links. Scheduled commercial banks accounted for 69% of the attacks, with urban co-operative banks and non-banking finance companies reporting 19% and 12% of the incidents, respectively

The Most Common technique of the Cyber Attacks:

Although there are numerous methods an attacker can use to breach an IT system, the majority of cyber-attacks typically follow comparable strategies. Below are a few of the most frequent types of cyber-attacks:

1. Malware,

Malware is any software created to harm a computer, server, or network. It can cause problems like leaking private information, allowing unauthorized access, blocking access to information, or interfering with a user's security and privacy without them knowing. Malware comes in different forms, such as computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wipers, and keyloggers[13].

Malware is a serious threat to both individuals and businesses on the internet. According to Symantec's 2018 Internet Security Threat Report, the number of malware types doubled from 2016 to 2017, reaching nearly 670 million. Cybercrime, including malware attacks, was expected to cost the global economy $6 trillion by 2021, and this figure is growing by 15% each year. Since 2021, some malware has been designed to attack systems that control critical infrastructure, like the electricity grid[14].

2. Hacking

The term "hacking" describes the unapproved use, alteration, or misuse of computer networks, software, or systems. To obtain illegal access to financial systems, cybercriminals use a variety of methods and instruments, including malware, spyware, and brute-force attacks. Once inside, they can use system vulnerabilities for nefarious reasons, alter transactions, disrupt services, or steal confidential information. For banks, hacking can result in significant monetary losses,

[13] Sharon Shea, Executive Editor., 12 Common Types Of Malware Attacks And How To Prevent Them Isabella Harford, Techtarget, 26 Jun 2024

[14] Neuhauser, Tanja Zseby & Joachim Fabini, Malware Propagation In Smart Grid Networks: Metrics, Simulation And Comparison Of Three Malware Types, Springer Nature Link, 28 August 2018

harm to their brand, and erosion of client confidence. Furthermore, ransomware attacks and other forms of cybercrime, such data breaches, might be preceded by hacking[15].

3. **worm**

A computer worm is a type of malware that copies itself and spreads to other computers without needing human action. It gets into devices by exploiting security flaws or through malicious links or files. Once inside, it looks for other connected devices to infect. Worms often go unnoticed by users because they hide as regular work files.

WannaCry is a famous example of a worm that also acts as ransomware. It spread by taking advantage of a weakness in older versions of Windows' Server Message Block (SMB) protocol. In its first year, WannaCry spread to 150 countries. By the following year, it had infected nearly 5 million devices[16].

4. Bots

A bot is a type of malware that replicates itself and spreads to other machines, forming what is known as a botnet—a network of bots. Devices that have been infected carry out automatic actions under the attacker's control. DDoS assaults frequently make use of botnets. They are also capable of sending phishing emails and keylogging[17].

A well-known example of a botnet is Mirai. This malware still targets IoT and other devices, having initiated a large DDoS attack in 2016. Studies also reveal that during the COVID-19 epidemic, botnet usage increased. The malware spreads to corporate systems through infected consumer devices, which are popular targets for Mirai and other botnets, that are utilised for work or on the networks of workers who work from home on company-owned devices.

5. keylogger

A keylogger is a type of spying malware that tracks what a person types on their keyboard. Hackers use keyloggers to steal usernames, passwords, and other sensitive information. Keyloggers can be either hardware or software. Hardware keyloggers are small devices that

[15] Mrudula Kuchi , Cybercrime and its impact on the banking industry, I pleader, October 12, 2023

[16] Sharon Shea, Executive Editor and Isabella Harford, 12 common types of malware attacks and how to prevent them, TechTarget, Published: 26 Jun 2024

[17] ibid

are attached to keyboards, and attackers must physically collect the device later to get the data. Software keyloggers don't need physical access; they are usually downloaded by victims through harmful links or email attachments. These software keyloggers record everything typed and send it to the hacker.

Agent Tesla is a well-known keylogger that was first seen in 2014. It's still a problem today, with newer versions not only tracking keystrokes but also taking screenshots of the victim's device. Using password managers can help protect against keylogger attacks because they automatically fill in usernames and passwords, so there's nothing for the keylogger to record[18].

6. Spyware

Spyware is harmful software that secretly downloads onto a device without the user knowing. It steals personal information, like passwords and bank details, and sells it to advertisers or other parties. Spyware infects devices through bad apps, links, websites, or email attachments. On mobile devices, spyware can spread through text messages and is especially dangerous because it can track a user’s location and access the device's camera and microphone. Different types of spyware include adware, keyloggers, Trojans, and mobile spyware.

Pegasus is a type of mobile spyware that attacks iOS and Android devices. It was first discovered in 2016 and was connected to the Israeli tech company NSO Group. In November 2021, Apple sued the company for targeting Apple customers and products. Pegasus was also linked to the murder of Saudi journalist Jamal Khashoggi in 2018[19].

7. Trojan horse

A Trojan horse is a type of harmful software that tricks users by pretending to be legitimate. It uses social engineering to get into devices. Once inside, it installs harmful code, known as the payload, to carry out the attack. Trojans can allow attackers to secretly access the device, track what the user types, install viruses or worms, and steal data.

[18] ibid

[19] Ibid

Remote Access Trojans (RATs) let attackers take control of an infected device. Once they have control, they can use the infected device to spread the Trojan to others and create a network of controlled devices, called a botnet[20]

8. Phishing

Cybercriminals utilize phishing, a dishonest tactic, to steal sensitive data including passwords, usernames, and debit/credit card numbers. Attackers deceive people into divulging their personal information by assuming the identity of reliable organizations, frequently through emails or phony websites. Phishing is particularly dangerous in the banking sector since it targets both staff and clients of the bank and can result in identity theft, fraudulent transactions, and illegal access to bank accounts. Over time, phishing attempts have changed as cybercriminals have become more skilled in their techniques, making it difficult for even the most watchful users to discern between genuine and fake messages[21].

9. Ransomware

Malicious software that encrypts a victim's data and requests payment in exchange for the decryption key is known as ransomware. Ransomware is a serious danger to the banking sector since it can completely shut down a bank's operations by making vital data inaccessible. Ransomware is a tactic used by cybercriminals to target banks and their clients, with the potential to result in large financial losses, interruptions to business as usual, and long-term harm to the bank's reputation. Since ransomware can have disastrous effects from even one successful attack, financial institutions are facing one of their biggest cybersecurity challenges due to the current surge in ransomware attacks[22].

Legal Provision For Cyber Attack In India

Information Technology Act, 2000 (IT Act) and other relevant legislation are the main legislative frameworks that regulate cybersecurity and cyberattacks in India. For the purpose of addressing new cybersecurity concerns, the Information Technology (Amendment) Act of 2008 revised the IT Act. Some of India's most important cyberattack laws are listed below:

[20] ibid

[21] Mrudula Kuchi, Cybercrime and its impact on the banking industry, I pleader, October 12, 2023

[22] ibid

1. Information Technology Act, 2000

1) Section 66: Deals with computer-related offenses such as hacking, unauthorized access, and data theft. Penalty includes imprisonment up to 3 years or a fine up to Rupees 5 lakhs, or both.
2) Section 66B: Punishes the dishonestly receiving of stolen computer resources or communication devices with imprisonment of up to 3 years or a fine up to Rupees 1 lakh.
3) Section 66C: Penalizes identity theft, where a person fraudulently uses another person's digital signature, password, or other unique identification features. Punishment includes imprisonment up to 3 years and a fine of Rupees 1 lakh.
4) Section 66D: Covers cheating by impersonation using a computer resource, with imprisonment up to 3 years and a fine up to Rupees 1 lakh.
5) Section 66E: Penalizes the violation of privacy through the capture, transmission, or publication of images of a person's private parts without consent, with imprisonment up to 3 years and a fine up to Rupees 2 lakh.
6) Section 66F: Addresses cyber terrorism, which involves acts that threaten the unity, integrity, security, or sovereignty of India by causing damage to critical information infrastructure. It carries imprisonment for life.

2. Indian Penal Code, 1860 (IPC)

1. Section 463: Relates to forgery, which includes creating false electronic records. Punishment includes imprisonment for up to 2 years or a fine.
2. Section 465: Provides for punishment of forgery (including cyber forgery) with imprisonment up to 2 years or a fine or both.
3. Section 468: Addresses forgery for the purpose of cheating, punishable with imprisonment up to 7 years and a fine.
4. Section 471: Covers using forged documents or electronic records as genuine, with similar penalties as forgery.

3. Critical Information Infrastructure Protection

Section 70 of the IT Act protects Critical Information Infrastructure (CII). Any unauthorized access or attempt to secure access to CII is punishable with imprisonment of up to 10 years and a fine.

4. Cert-In (Indian Computer Emergency Response Team

Under Section 70B of the IT Act, CERT-In is responsible for incident response, including cybersecurity incidents. It monitors and responds to cyber threats, and organizations are required to report cyber incidents to CERT-In.

5. Rules under the IT Act

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: These rules set out due diligence requirements for intermediaries and social media platforms, making them responsible for the content hosted on their platforms.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: Provide guidelines for the protection of sensitive personal data, including in cases of data breaches.

6. Other Provisions

Section 72: Penalizes the breach of confidentiality and privacy with imprisonment for up to 2 years or a fine of up to Rupees 1 lakh, or both.

Section 43A: Mandates organizations handling sensitive personal data to implement "reasonable security practices" and to be held liable to pay damages for failure in protecting such data.

7. Data Protection Bill

India is also in the process of implementing a Personal Data Protection (PDP) Bill, which aims to enhance data privacy and security by regulating the collection, processing, and storage of personal data.

These legal frameworks aim to address the growing threat of cyber crimes and ensure a robust response to cyber attacks in India.

Suggestion To Prevent Cyber Attack

Preventing cyberattacks is crucial for any country, especially India, which is quickly becoming a leader in digital technology. As technology use increases, so does the risk of cybercrimes, making it essential to take strong steps to ensure cybersecurity. Here’s how India can work to prevent cyberattacks:

1. Improving Cyber Laws

India’s cybercrime laws must keep up with fast-changing cyber threats. The Information Technology Act of 2000, which governs cybercrime, needs regular updates to address new challenges like data theft, cryptocurrency scams, and cyber spying. Strict penalties and quick legal action can help deter potential cybercriminals. Working with other countries on cyber law enforcement is also important for dealing with international cybercrimes.

2. Raising Public Awareness about Cyber Hygiene

Educating the public on basic cybersecurity practices is a powerful way to prevent cyberattacks. Promoting the use of strong passwords, multi-factor authentication, and secure internet habits can greatly reduce risks. Government programs like Digital India should include cybersecurity awareness to reach people across urban and rural areas, where digital literacy may be lower.

3. Strengthening Infrastructure Security

India’s essential infrastructure, like power grids, transportation, and banks, are often targets for cyberattacks. Securing these areas requires using advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML) to detect threats in real time. Adopting specific cybersecurity guidelines for each industry will also help protect important infrastructure from complex attacks.

Encouraging Public-Private Collaboration

Cybersecurity is not just the government’s job. Private companies, especially tech firms, play an essential role in preventing cyberattacks. Public-private partnerships can help share information on potential threats, create new security technologies, and set up quick response teams when there’s a security breach. Platforms like Cyber Swachhta Kendra (Cyber Hygiene Centre) are good examples and should be expanded.

Building a Skilled Cybersecurity Workforce

India needs more trained cybersecurity professionals to handle the growing threat landscape. The government and schools should work together to offer specialized cybersecurity courses, certifications, and career opportunities. With a skilled workforce in ethical hacking, network security, and forensics, India can improve its defenses against cyber threats.

Enhancing Incident Response and Recovery

Even with strong security, some cyberattacks may still happen. India needs a good system in place for responding to attacks. This includes setting up Computer Emergency Response Teams (CERT-In) and ensuring that all important institutions have a well-practiced recovery plan. Quick response times can reduce an attack's impact and help things return to normal faster.

Increasing Global Cooperation on Cybersecurity

Cyber threats cross borders, so fighting them needs global cooperation. India should actively participate in international forums like the United Nations and Interpol to share knowledge, best practices, and ways to handle threats. Partnering with global tech giants and cybersecurity companies can also strengthen India's ability to counter complex cyber threats from around the world.

Conclusion

As India develops its digital infrastructure, cybercrime has grown to be a serious menace to the nation. The development of the internet has created many chances for advancement, but it has also made flaws more visible, which hackers take advantage of. Cyberattacks come in a variety of forms, from Malware, worm, Hacking, Bots, and others. These attacks have dire repercussions, including monetary losses, identity theft, and interruptions to vital services. The critical need for enhanced cybersecurity measures is highlighted by high-profile instances like the cyberattack on AIIMS Delhi and data breaches affecting millions of Indians.

With the help of legislative frameworks like the Indian Penal Code (IPC) and the Information Technology Act of 2000, India has achieved progress against cybercrime. The Indian Computer Emergency Response Team (CERT-In) was also founded by the government to keep an eye on and address cyberthreats. The frequency and sophistication of cyberattacks continue to escalate in spite of these efforts, mostly as a result of nation-state actors and organised crime syndicates taking advantage of holes in the system. The dark web gives thieves a venue to exchange malware and attack services, which makes enforcement even more difficult.

India came in fifth place in the world in 2023 with 5.3 million compromised accounts, serving as a sobering reminder of the issue's expanding scope. To secure India's digital ecosystem, much more work needs to be done, even though initiatives like the forthcoming Data safety Bill seek to strengthen the safety of personal data.

A number of tactics can be used to lower the danger of cyberattacks. Enhancing infrastructure security and fortifying the country's cybersecurity architecture are essential. Reducing cyber dangers will also be largely aided by strengthening cyber legislation, educating the public about cyber hygiene, and promoting public-private cooperation. To keep abreast of new dangers, cybersecurity research must be supported and a devoted personnel in place. Furthermore, because they are frequently the targets of cyberattacks, small and medium-sized businesses (SMEs) require extra protection. Given the cross-border nature of cybercrime, international cooperation is also required.

India has to keep improving its institutional and legislative responses to cybercrime while closely collaborating with other nations to exchange resources and expertise. In order to reduce the impact of cybercrime in the upcoming years, it will be imperative to develop a strong cybersecurity infrastructure and encourage a culture of cyber cleanliness among residents. Protecting the country's digital assets and ensuring its future in the digital era ultimately necessitates a multifaceted approach encompassing all spheres of society, from corporations and government to citizens.