Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April-2025 | Page 159-169

THE IMPACT OF TECHNOLOGY ON THE RISE OF CYBERCRIME

[1]Akansha Kujur, [2]Anjali Sahu, [3]Rishita Udde
[1,2]Student of BALLB 10th Semester
[3]Student of BBALLB 10th Semester
Kalinga University, Raipur, Chhattisgarh

Abstract:

In today's world, technology has become an increasingly important part of our lives. Modern technology has transformed how societies function, allowing for faster communication, more effective commercial operations, and easy access to information. However, as technology has advanced, cybercrime has increased, posing severe hazards to individuals, businesses, and governments around the world. Technological advancement has both beneficial and harmful consequences. One of the negative consequences of the advancement of information technology is the misuse of the information technology, which can hurt others. With the rise of the internet, mobile devices, cloud computing, and artificial intelligence, the digital world has expanded dramatically, opening up new opportunities for cybercriminals. Phishing, identity theft, ransomware, online fraud, and data breaches are examples of the sophisticated digital versions of traditional crimes. Cybercriminals use flaws in hardware, software, and human behaviour to obtain sensitive information without authorization or interfere with necessary services. Cybercrime is more alluring and challenging to track down because of the anonymity provided by internet and the capacity to operate internationally. The widespread use of insecure digital platforms, as well as poor cybersecurity policies, are major factors to the development of cybercrimes. As more personal and financial information is stored online, criminal actors have a larger attack surface. Furthermore, the dark web has enabled the anonymous trading of unlawful products and services, such as hacking tools and stolen data, exacerbating cybercriminal activity. The fast growth of technologies such as the Internet of Things (IoT), machine learning, and blockchain has created new cybersecurity challenges. These technologies provide complicated security threats in addition to their many advantages. IoT devices, for example, frequently have weak security measures, which leaves them vulnerable to abuse. Similar to this, artificial intelligence can be used to produce convincing deepfakes or automate cyberattacks, making it more difficult to discern between malicious and legitimate behaviour.

Keywords: Information Technology, Internet of Things, Cybercrime, ransomware, cybersecurity, digital threats.

Introduction:

Information technology is constantly evolving. Over the last few decades, technological innovation has transformed practically every area of human life. Digital technology is now deeply established in modern society, affecting everything from personal communication and financial transactions to national security and global trade. The internet, in particular, has transformed how people connect, do business, and obtain information. Along with these favourable advancements, there has been a big and growing drawback: the rise of cybercrime. As technology advances, cybercriminals' methods and plans improve, posing increasingly sophisticated risks to individuals, companies, and governments. Cybercrime, defined as criminal behaviour involving a computer, networked device, or network, has grown in scope and complexity. With the rise of smartphones, cloud computing, social media, and the Internet of Things (IoT), there is more data being generated and saved online than ever before. Massive prospects for both innovation and exploitation have been made possible by this digital revolution. With the use of sophisticated tools, hackers and cybercriminal groups can now evade conventional security measures and steal personal information, embezzle money, disseminate false information, and even bring down vital infrastructure. Cybercrime's development can be linked to the early days of computing, when harmful activity was primarily restricted to digital graffiti or practical jokes. However, as the global economy grew more digital and the internet became more commercialized, cybercrime swiftly became a very lucrative business. These days, ransomware is frequently used by hackers to extort millions of cash from companies, or by state-sponsored organizations to conduct cyberattacks for strategic or political objectives. As a result, with consequences for national security, economic stability, and privacy, cybercrime has emerged as one of the most urgent issues of the digital age. Cybercrime remains a growing danger despite greater knowledge and investments in cybersecurity. The sheer nature of technology presents some of the problem; its quick speed of development frequently surpasses the capacity of legal, regulatory, and enforcement systems to keep up. It is also very challenging to detect, attribute, and prosecute cybercriminals due to the anonymity offered by the internet and the worldwide scope of cyber networks. Unquestionably, technology has improved society, but it has also greatly accelerated the growth and development of cybercrime by increasing the attack surface, opening up new avenues for criminal activity, and surpassing the pace at which appropriate security and legal safeguards have been put in place.

What is Cybersecurity?

Cybersecurity is the process of defending programs, networks, systems, and data from online threats, illegal access, and harm. It is essential to maintain data availability, confidentiality, and integrity in today's digitally driven world, when government, business, and personal data are all kept and transferred electronically. It is a broad category of tactics and tools used to protect digital assets. They consist of intrusion detection systems, firewalls, antivirus programs, encryption, multi-factor authentication, and secure coding techniques. Preventing online dangers including ransomware, phishing, malware, data breaches, and denial-of-service assaults is the aim.

One critical part of cybersecurity is finding and controlling system vulnerabilities before they can be exploited. This involves frequent updates, patch management, and risk assessments. Furthermore, as cyber threats grow in complexity and size, cybersecurity evolves by adding artificial intelligence (AI), machine learning, and behavioural analytics to better forecast and prevent assaults. It is a dynamic and essential discipline that protects our digital lives. As technology continues to advance, the importance of robust cybersecurity measures becomes increasingly significant. It is not only about defending against attacks but also about creating a secure digital environment.

Understanding The Concept of Cybercrime and Cyber Attacks:

One of the types of criminal behaviour that has grown the quickest in recent years is cybercrime. The prospects for cybercriminals have increased as digital technology develops more and internet use becomes more ingrained in daily life. The extent and consequences of cybercrime have significantly increased, impacting not just individuals but also businesses, governments, and organizations. These include financial fraud, identity theft, ransomware attacks, and data breaches.

Cybercrime:

Cybercrime refers to any illegal behaviour involving a computer, networked device, or network. Some cybercrimes, like hacking or virus attacks, target computer systems directly, while other cybercrimes, like fraud or stalking, use the internet to carry out traditional crimes. These offenses can be broadly divided into three categories: Crimes against people, such as phishing, identity theft, and online harassment, property-related crimes, including ransomware attacks, cyber fraud, and intellectual property theft, crimes against society or the government, such as disseminating propaganda, hacking government networks, and cyberterrorism. Cybercrime has increased alarmingly over the past ten years, and hackers are using increasingly advanced methods and resources. This trend was expedited by the COVID-19 pandemic in 2020, as greater online activity and remote work increased vulnerability. Cybercriminals used the epidemic to launch a larger-scale campaign of ransomware, phishing, and frauds, according to INTERPOL and other cybercrime monitoring agencies.

The Norton Cyber Safety Insights Report estimates that in 2023, cybercrime impacted over 330 million people worldwide. According to Cybersecurity Ventures, the yearly cost of cybercrime is expected to exceed $10.5 trillion worldwide by 2025. In 2022, the National Crime Records Bureau (NCRB) stated that there were 65,893 cybercrime cases in India, a significant increase over the 50,035 cases reported in 2020. Over 8% of all registered IPC (Indian Penal Code) crimes are thought to be cybercrimes, which has steadily increased in India in recent years. In India, there were 4.8 cybercrimes for every lakh people in 2022.

Cyber Attack:

The term "cyber-attack" refers to any attempt by hackers or cybercriminals to access a computer system, network, or digital data without authorization and with harmful intent. Reputational harm to persons and organizations, financial loss, service interruption, and data theft are all possible outcomes of these attacks. Man-in-the-middle attacks, ransomware, malware infections, Distributed Denial of Service (DDoS) assaults, and phishing are examples of common cyberattacks. In recent years, cyberattacks have taken centre stage as a major type of cybercrime, accounting for around 40% of all cybercrimes worldwide. Without the adoption of strong cybersecurity procedures, the scope, scale, and effect of cyberattacks are anticipated to expand further due to the rapid advancement of technology. To create a secure digital ecosystem, governments, businesses, and individuals must collaborate by making investments in cybersecurity infrastructure, increasing public awareness, and implementing stronger cyber laws. The only effective way to combat the growing threat of cyberattacks is to work together.

Effects of Cyber Attacks and Their Share in Cybercrime:

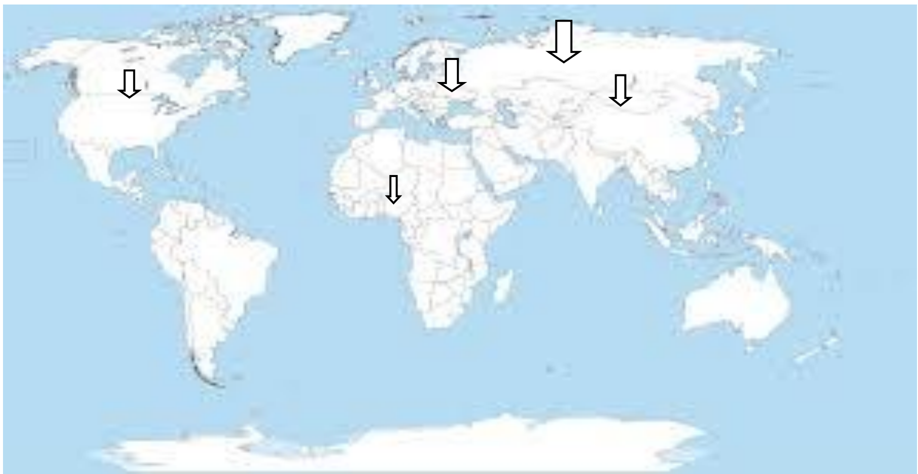
In today's digital era, the growth of technology has provided enormous benefits to individuals, corporations, and governments. However, this digital dependence has also given rise to a new threat: cyber-attacks. These attacks have become a significant part of cybercrime, affecting millions of people and companies worldwide.

Effects of Cyberattacks:

Cyberattacks can have disastrous results, and they fall into one of the following categories: 1. Financial Effects: Worldwide, cyberattacks have resulted in damages worth trillions of dollars. In addition to direct financial losses (from theft, ransomware, or outages), businesses often suffer indirect financial losses from: productivity loss as a result of damaged systems, Damage to one's reputation that results in a decline in business, Investigative and legal fees Recovery and security upgrade costs.

2. Sensitive Information Loss and Data Breach: The goal of many cyberattacks is to steal private information, whether it be financial, personal, or business-related. These security lapses may reveal: Records of customers, Intellectual property, Secrets of the government, Health care records, Identity theft, illicit financial transactions, and even threats to national security result from this.

3. Threats to National Security: State-sponsored cyberattacks target government networks, defence systems, and infrastructure. Attacks of this nature have the potential to jeopardize national security, provoke geopolitical unrest, and potentially qualify as war crimes. A case in point is the Stuxnet malware, which allegedly interfered with Iran's nuclear program, demonstrating the tangible effects of cyberattacks.



1. Russia 58.39%

2. Ukraine 36.44%

3. China 27.86%

4. United States 25.01%

5. Nigeria 21.28%

Note: Percentage of data provided according to the World Cybercrime Index.

Fig. 1Top five countries identified as the most significant sources of Cybercrime globally.

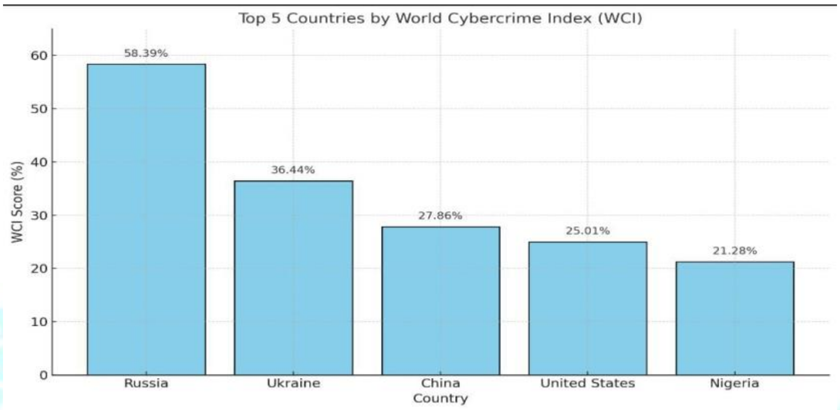


Fig 2. The Graph shows the cybercrime in various countries (2024)

Fig. 2 Shows the data according to the World Cybercrime Index published in April 2024.[1]

Cyber Attacks and Their Share in Cybercrime:

One of the main elements of cybercrime is cyberattacks. Although cybercrime encompasses a wide range of illicit online behaviours, cyberattacks are the most technically intricate and significant type of cybercrime. Let's examine their role and share:

1. Increased Market Share: Over 60–70% of cybercrime events involve some kind of cyberattack, according to international cybersecurity reports (such as those from IBM, Norton, and McAfee). The rising number of susceptible devices linked to the internet and the expanding usage of digital services are the main causes of this high percentage.
2. Utilization in Multi-Layer Cybercrime: The beginning of many cybercrimes is a cyberattack. As an example: Ransomware can be installed using phishing emails, and the malware can subsequently be used to extort money. Attackers may utilize malware infections to eavesdrop on users and take information for malicious purposes. Cyberattacks

[1] https://www.ndtv.com/world-news/russia-on-top-of-global-cybercrime-index-read-where-india-stands-5419575?utm_source=chatgpt.com

are essentially the vehicle via which a variety of other crimes, such as financial fraud, extortion, and blackmail, are delivered or entered.

3. A Higher Level of Complexity: Advanced social engineering, deepfakes, and artificial intelligence are all being used in increasingly complex cyberattacks. Traditional cybercrime is developing into intricate attack-based frameworks as criminals embrace new technology, making cyberattacks an even more prominent aspect of the contemporary cybercrime environment.

In 2022, the states with the highest number of reported cybercrime cases were:

- Telangana: 15,297 cases
- Karnataka: 12,556 cases
- Uttar Pradesh: 10, 117 cases

These three states accounted for the significant portion of the total cybercrime cases reported in India.[2]

Numbers of Cybercrime related to social media:

In 2021 and 2022, India experienced a major increase in the rate of cybercrime cases registered under the Information Technology (IT)Act and the Indian Penal Code (IPC). According to the National Crime Bureau Records (NCRB), cybercrime cases rose from 52,974 in 2021 to 65,893 in 2022, making a 24.4% increase. Majority of the cases were related to fraud, accounting for 64.8% (42,710 cases) in 2022. Other cases included extortion (5.5%) and sexual exploitation (5.2%). While the number of arrests related to cybercrime cases was substantial 25,799 in 2022 and the conviction rate remained low with only 1,407 individuals convicted that year.[3]

Cybercrime	Cases in 2020	Cases in 2024
Fake or Impersonating profiles	12,310	39,846
Profile Hacking and Identity Theft	10,419	38,295
Cyberbullying and Stalking	11,641	39,007
Cheating by Impersonation	9,808	19,989
Online Job Fraud	4,973	10,461

Fig. 3 Key Trends in social media related Cybercrimes

Effectiveness of the Information Technology Act, 2000 in the Prevention of Cybercrimes:

[2] https://www.etvbharat.com/english/bharat/cybercrime-cases-on-the-rise-in-country-says-minister-of-state-for-home/na20231212184047633633062?utm_source=chatgpt.com

[3] https://www.etvbharat.com/english/bharat/cybercrime-cases-on-the-rise-in-country-says-minister-of-state-for-home/na20231212184047633633062?utm_source=chatgpt.com

In order to enhance electronic governance and give legal status to electronic trade, India passed the Information Technology Act, 2000, also known as the IT Act. But as the danger of cybercrimes has grown over time, the Act has also emerged as a key legal weapon to stop online transgressions. Although it established the structure for India's cyber law, the IT Act has drawn praise and criticism for its ability to deter cybercrimes.

Strengths of the IT Act in Cybercrime Prevention:

1. The legal recognition of a variety of cybercrimes is one of the main accomplishments of the IT Act. Hacking (Section 66), identity theft (Section 66C), cyberterrorism (Section 66F), and the publication of pornographic material in electronic form (Section 67) are among the offenses that have been covered by it as punishable crimes. Law enforcement agencies are now able to combat digital misdeeds that were previously un-addressable by conventional legislation.
2. Amendments to Address Changing Threats: The IT Act was amended in 2008 to include new clauses addressing child pornography, phishing, spam, data breaches, and cyberstalking. Because of these modifications, the law is now more resilient and adaptable to the changing nature of cyberthreats.
3. Facilitation of Adjudication and Investigation: The Act also establishes cyber appellate tribunals and appoints adjudicating officers to facilitate investigation and adjudication. This has made it easier to settle conflicts more quickly and, in some situations, implement sanctions.
4. Enabling Law Enforcement Powers: The government and its agencies are empowered to monitor, intercept, and decrypt any information for the sake of security and inquiry by virtue of sections such as 69 and 69B. Tracking down cybercriminals and averting possible dangers has been made possible by this clause.
5. Data Protection Provisions: Under Section 43A of the IT Act, businesses that handle private information are required to put in place appropriate security measures. This clause incentivizes proactive cybersecurity activities and discourages carelessness in data protection.

The IT Act of 2000 was a first move in establishing a legal framework to combat cybercrimes in India; nevertheless, its efficacy is constrained by out-of-date provisions, lax enforcement, and new types of digital offenses. A more thorough and specialized legal framework is desperately needed in the quickly evolving digital world of today. Modern laws are being introduced with the Digital Personal Data Protection Act, 2023, and current debates about the Digital India Act. Improved data security, digital platform responsibility, and more precise rules for prosecuting cybercrimes are the goals of these proposed reforms. The government must also fund cyber awareness initiatives, upgrade law enforcement's digital infrastructure, and foster international collaboration in order to increase the IT Act's efficacy in deterring cybercrimes. In the digital age, cybercrimes can only be successfully prevented and prosecuted through a multifaceted and flexible approach. Additionally, the cyber regulations significantly affect India's emerging economy and online businesses. Therefore, it's critical to comprehend the IT Act of 2000's many views and what it has to offer.

There are several laws and policies that penalize cybercrime. Nonetheless, practically all of the restrictions are derived from the Information Technology Act (IT Act), 2000, and the Indian Penal Code (IPC), 1860. India's general penal code, or IPC, lists offenses and their associated punishments. The IPC, which has been revised legally and is prudently regarded as enforceable against cybercriminals, includes real-world rules and penalties. In contrast, the IT Act is a specific law that deals with the use of information technology and offenses involving it. 2008 saw the passage of the IT Amendment Act, which covers a number of cybercrimes. The IT Act and IPC complement one other when it comes to cybercrime against women.

Better Solutions to Overcome the Challenges and Minimize the Cybercrimes:

One of the biggest risks in the contemporary digital environment is cybercrime. The internet's extensive use and the quick development of technology have made people far more vulnerable to cyberattacks. Hacking, phishing, identity theft, cyberbullying, ransomware assaults, and other malevolent actions carried out through digital channels are examples of cybercrimes. Potential targets include individuals, groups, and governments. Strong solutions are desperately needed to lessen the hazards posed by hackers as their tactics change. This addresses the main obstacles to stopping cybercrime and offers all-encompassing ways to reduce its incidence.

Challenges in Combating Cybercrimes:

1. Evolving Nature of Threats: Cybercriminals are always creating new tools and methods in response to security measures. Security systems find it challenging to stay up to date with the ever-changing threats, which range from sophisticated ransomware to zero-day attacks.
2. Insufficient Knowledge: The general lack of user understanding regarding cyber hygiene is one of the biggest problems. Because they don't know how cybercriminals work, a lot of individuals fall for scams.
3. Insufficient Lawmaking and Implementation: Comprehensive cyber laws and the necessary infrastructure are lacking in many nations. The global nature of the internet makes jurisdictional difficulties a significant obstacle to prosecuting perpetrators, even in cases where laws are in place.
4. Lack of Qualified Professionals: Globally, there is a serious lack of cybersecurity experts. In this industry, the mismatch between supply and demand leads to inadequate system and network protection.
5. Misuse and Privacy of Data: It is getting harder to protect privacy and stop data misuse as more information is gathered and kept online. Sensitive data is not adequately protected by many organizations.
6. Absence of Global Collaboration: Cybercrime does not only occur in one nation. Attackers frequently use procedural and legal variations to conduct their operations internationally. International agencies' inability to coordinate makes it more difficult to investigate and prosecute cybercriminals.

Better Solutions to Minimize Cybercrimes:

To effectively counter cybercrime, a multi-layered and collaborative approach is required, combining legal, technical, organizational, and educational strategies.

For enhancing legal structures governments must make sure that their legal systems are up to date with the latest developments in technology. Laws must be all-encompassing and address new risks like deepfakes, cryptocurrency fraud, and cyberattacks powered by artificial intelligence. To discourage potential perpetrators, cybercrimes should carry harsher punishments. Creating courts specifically designed to handle cybercrimes helps speed up proceedings and guarantee that the judiciary has a thorough understanding of technical matters. By strengthening the infrastructure for cybersecurity, the use of artificial intelligence (AI) and machine learning is very important. These tools can instantly identify dangers before they cause harm by analysing trends and spotting abnormalities. Businesses should utilize "zero trust" security models, in which all access requests are validated regardless of the user's location. Regular audits can assist in locating vulnerabilities and applying the required fixes.

Building Capacity and Training for development of a Skilled Workforce to close the skills gap, further cybersecurity, ethical hacking, and information security courses should be offered by academic institutions. Partnerships between the private sector, academics, and governments can improve collective security and stimulate innovation. Companies need to provide frequent cybersecurity education to their employees on how to identify threats and follow cybersecurity procedures. Strengthening Mechanisms for Incident Response with a Specialized Cybersecurity Response Teams to guarantee a prompt and well-coordinated reaction to cyber incidents, CERTs (Computer Emergency Response Teams) should be established at the national and organizational levels. Cyber Drills and Simulations: Regularly conducting cyber drills aids in evaluating preparedness and locating response strategy flaws. Portals for Incident Reporting: Victims should have access to user-friendly tools that enable them to promptly report cybercrimes.

Cybercrimes often involve perpetrators located in different geographic locations, which can create challenges in determining jurisdiction and initiating legal action. Cooperation and coordination between different law enforcement agencies, both within India and internationally, are essential. Encouraging Global Collaboration for Global Treaties and Agreements for combating cross-border cybercrimes requires international cooperation. It is important to enact and reinforce agreements like the Budapest Convention on Cybercrime. Nations should create avenues for exchanging up-to-date intelligence on criminal activity and cyberthreats. Facilitating the quicker extradition of cybercriminals can strengthen the international legal system's deterrent power. And for Protecting Vital Infrastructure Special Protection Measures shall be taken. Strong cybersecurity procedures are required to safeguard energy grids, transportation networks, financial institutions, and healthcare services. These provide service continuity even in the case of a cyberattack. Regulators are responsible for making sure operators of vital infrastructure adhere to cybersecurity guidelines. Using a Blockchain Technology in Cybersecurity Immutable Data Storage by producing tamper-proof records, it can assist in protecting sensitive data and transactions. Decentralized identity systems can shield users against fraud and identity theft. By implementing preset guidelines, Smart Contracts and procedures, they can improve the security of online transactions.

Conclusion:

All of the above discussion shows that technology has both pros and cons for individuals, societies, governments and economies to the great extent. Because cybercrime is a dynamic and complicated danger, a multifaceted, coordinated response is necessary. The speed at which technology is developing has unquestionably changed how we manage information, interact, and do business. Although there are many advantages to these developments, they have also created a frightening new problem: cybercrime. As technology advances, cybercriminals' tactics and level of expertise also change. The growth of digital platforms and the internet has increased the attack surface for cybercriminals. In several domains, technological developments have also surpassed the creation of cybersecurity solutions. Because of a lack of awareness, inadequate infrastructure, or a lack of money, organizations frequently find it difficult to stay on top of developing dangers. Meanwhile, to launch increasingly focused and potent attacks, cybercriminals use encryption, machine learning, and artificial intelligence. It has several initiatives to monitor, control cybercrimes including Information Technology Act 2000. However, taking the changing nature, forms and dimensions of cybercrimes into account, it needs more deep level and strict provisions. Ultimately, although technology has sparked advancement, it has also unintentionally contributed to the rise in cybercrime levels. Resolving this issue calls for a well-rounded strategy that encourages technical innovation while maintaining security, alertness, and ethical online conduct. Our best chance of reducing the threats and creating a safer online environment for everybody is if we work together.

References:

1. https://online.ucpress.edu/gp/article/2/1/27353/118411/How-Is-Technology-Changing-the-World-and-How
2. https://www.jsr.org/index.php/path/article/view/2284
3. https://www.researchgate.net/publication/365421976_Organisational_Changes_in_the_Age_of_Digital_Transformation
4. https://community.nasscom.in/communities/it-services/information-technology-and-its-role-indias-economic-development
5. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
6. https://cdn.visionias.in/value_added_material/00381-various-security-forces-and-agencies-and-their-mandate_economy.pdf
7. https://www.researchgate.net/publication/377957344_COMPREHENSIVE_REVIEW_ON_CYBERSECURITY_MODERN_THREATS_AND_ADVANCED_DEFENSE_STRATEGIES
8. https://www.statista.com/statistics/617136/digital-population-worldwide/
9. https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/
10. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full
11. https://sosafe-awareness.com/glossary/quid-pro-quo-attacks/

12. https://tdsat.gov.in/admin/introduction/uploads/INFORMATION%20TECHNOLOGY%20ACT.pdf
13. https://www.researchgate.net/publication/386327138_Emerging_technologies_and_cyber-crime_strategies_for_mitigating_cyber-crime_and_misinformation_on_social_media_and_cyber_systems
14. https://indonet.co.id/factors-causing-cyber-crimes-to-easily-occur/
15. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.pdf
16. https://pmc.ncbi.nlm.nih.gov/articles/PMC10123536/