INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 1 - V8I1-1151)
Available online at: https://www.ijariit.com

The present and future trends of cybercrimes

Ravichandran Ramasamy
lionravichandran@gmail.com
Livingstone International University of Tourism Excellence and Business Management, Lusaka, Zambia

ABSTRACT

There have been many challenges today amongst the organizations and the governments to achieve a more secure digital environment. Recent pandemic has paved way to cybercriminals a unique opportunity to penetrate human defences. The present day cyberattacks become highly sophisticated and much more dangerous. Data leakage continues to be a significant threat by working remotely, the cost of defending the breaches has risen to a new high. The present-day cyber-attacks shows not just data theft, they are acting in a catastrophic manner by intruding into the essential infrastructures like hospitals, gas pipelines, electricity, and water supply leading to serious physical harm. Tessian cybercrime statistics says, "Google has registered 2,145,013 phishing sites as of January 17, 2021. This is up from 1,690,000 on January 19, 2020. (27% increase in a year). Ransomware is prevalent in 2021. Data exfiltration is now a big part of the game with what is called double extortion ransomware.Trend Micro alone detected 34% more new ransomware families in 2021than last year" (1). Apart from the present-day cybercrimes, newer forms of cyber threats are evolving every day. Cyber threat statistics shows that there are many emerging threats like, Ransomware attack using data exfiltration, Cryptojacking, Mobile spywares, IoT focused cybercrimes, 5G based intrusion, Stalkerware, irreparable malware attacks, and State sponsored Cyberactivism. As technology is growing at a rapid pace, the present-day cyber criminals make use of every technological development for their criminal activities. The purpose of this article is to understand the modalities of present forms of cybercrimes and evolution of new cybercrime trends of the near future.

Keywords: *Cybercrime, Cyberstalking, Denial of Service, DDoS, Cyber Defamation, Cyber Fraud, IPR Violation, Web Jacking, Crypto Jacking, Ransomware, Cyber Activism, Phishing, Data Exfiltration, Artificial Intelligence & IoT attacks.*

1. INTRODUCTION

As per Arthur J Gallagher, "Cybercrime is not going to go away, and as technology evolves criminals are also getting more and more inventive. Cybercrime levels are likely to get worse before they get better, and you need to take measures to protect yourself. Ground-breaking technology is being released all the time. Now is the time to undergo a thorough review of your current cyber security procedures, identifying any vulnerabilities. With the rise of the Internet of Things, it's no longer enough to secure laptops and smartphones and you need to consider anything with internet capabilities. Cyber-attacks are no longer just a possibility, they are an inevitable part of running your organization. A robust cyber policy can help to protect your business, managing the reputational damage and financial burden these attacks can generate."

Trend Micro has announced that they have identified 62.6 billion email born threats in 2020, which is almost 119,000 threats per minute. It also detected ransomware attack has been increased to 34% compared to last year. Tech Republic has told, "Unfortunately, COVID has given rise to many COVID-themed online threats. Around 25% of COVID-related domains are malicious". (2) Malware- as-a-Service (MaaS) is a new avenue of business, MaaS providing organizations rent malware to their customers on a subscription basis. They even regularly update their malwares as that of legitimate software applications. Now a days Internet of Things (IoT) becomes an essential business requirementfor any business. IoT brings agility and efficacy for the business processes. Tech analysts IDC predict "there will be 41.6 billion connected IoT devices worldwide by 2025". In fact, more and more IoT devices incorporated into the business process means more potentially vulnerable equipment and devices set in the business prone to cyberattacks anytime.

Data theft and leakage becomes a major threat for the organizations. Remote Desktop Protocol (RDP) attack, phishing and data-exfiltration are the innovative methods to gain access to systems and data bythe cyber criminals. Stalkerware is a software often installed on victims' devices unknowingly to traceall their activities. Organizations, even individuals become victims of the attack frequently. Cryptocurrency is now prevalent and slowly achieving global recognition. More and more people and organizations

started using it. Cryptocurrency being totally managed digitally, cybercrimes associated with cryptocurrency will be trending in future. Cryptojacking is a methodology that provides unauthorized access to the blockchain accounts and database that deal cryptocurrency or wallet, sothat the cybercriminal can steal the cryptocurrency or wallet money effortlessly. Projecting into the future cybercrimes require a complete understanding and strong assessment of current cyber threats and other key features of the cybersecurity ecosystem.

2. PRESENT DAY CYBERCRIMES

The present-day cybercrimes may be broadly classified under the following three categories:

(a) **Crime against Individuals** like E-mail related crimes, Cyber-stalking, Cyber Defamation, Unauthorized access, Email spoofing, Denial of Services attack, Cyber frauds & Cheating Vandalism, Malware attack by transmitting Viruses/Trojans/Worms, Intellectual Property Rights (IPR) violations and Telecom Frauds.

(b) **Crime against Organizations & Governments** like unauthorized access over computer system, Possession of unauthorized information, Malware attack by transmitting Viruses/Trojans/Worms, Intellectual Property Rights (IPR) violations and Telecom Frauds, Web jacking, Ransomware attack, Cyber terrorism against the government organization and Distribution of pirated software etc.

(c) **Crime against Society at large** like Pandemic related crimes, Pornography (child pornography), Illegal Trafficking, Financial crimes, Online gambling, and Supply chain attack.

Future trends of cybercrimes include Data Exfiltration, Blend of AI and IoT with 5G attacks, Cloud attacks, Cryptojacking, Irreparable Malware attack, Cyber Activism and Supply Chain Attack and many more. We will try to understand the present and future trends of cybercrimes, so that we will have a better and effective combating plans to survive digitally.

E-MAIL RELATED CRIMES: Email is one of the world's most preferred forms of communication. Billions of email messages travel around the globe daily. At the same time, Email is the most misused form of communications. Email is a powerful tool for cyber criminals. Emails are often the fastest andeasiest ways to propagate malicious code over the Internet. Some of the major email related crimes are harassment via threatening emails, email spoofing, sending malicious codes through email, email bombing, defamatory emails, and email frauds. Harassment through e-mails is not a new concept. It isvery similar to harassing through letters. A spoofed email is one that appears to originate from one source but has emerged from another source (3). The name and / or email address of the originator of the email usually falsified for email spoofing. Email spoofing is generally used to commit financial frauds. The person committing spoofing knows that there is no chance of being identified. Hence, email spoofing becomes popular methodology for cyber criminals. Kapurthala Police website indicated "Email Bombing refers to sending many emails to the victim's email account resulting inthe victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing" (4). There are many hacking tools available in the market to automate the process of email bombing. These tools send multiple emails at a same time from many different email servers to make victim's server flooded.

CYBER STALKING: The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking is defined as following a person's movements across the internet by posting messages (sometimes threatening), entering the chatrooms frequented, continuously disturbing the victim with false news, mails and messages. The famous antivirus provider, Kaspersky states "Cyberstalking can include other behaviour that's intended to intimidate victims or make their lives unbearable. For instance, cyberstalks might target their victims on social media, trolling and sending threatening messages; theymight hack emails, to communicate with the victim's contacts, including friends and even employers. Social media stalking can include faking photos or sending threatening private messages. Often, cyberstalks will spread malicious rumours and make false accusations, or even create and publish revenge porn. They might also engage in identity theft and create fake social media profiles or blogs about their victim" (5).

Cyberstalks use many types of techniques. These cyber criminals initially use internet to identify and explore victims' data. Then they send unsolicited e-mails, including hate, obscene or threateningmails and messages. They use live chat harassment to abuse the victim directly or through electronic sabotage. With social media, the cyberstalks create postings about the victim or start rumours and spread defamatory news or personal fictious information. Cyberstalks may also set up a web page on the name of the victim with false information for the purpose of discrediting the victim's reputation, posting false information about the victim, and soliciting unwanted contacts. Marshall.edu website states, "the rapidly advancing technology also makes it possible for abusers to use Spyware which is computer software or possibly a hardware device that allows someone to monitor and get information about someone else's computer use. The presence of the Spyware is usually totally unknown to the victim. Once installed, the Spyware can allow the abuser to monitor what is done on the computer, cell phone or other handheld devices. This is usually done remotely, so that the victim remains unaware that he/she is being monitored". (6)

UNAUTHORISED ACCESS: Unauthorised access, otherwise called as hacking is one of the most dangerous techniques. "Access" is defined in Section 2(1)(a) of the Information Technology Act as "entering, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network". However, unauthorised access refers to whena person gains entry to a computer network, system, application software, data, or other resources without permission of the owner of that information asset. Unauthorised access techniques include, packet sniffing, tempest attack, password cracking and buffer overflow. Packet sniffing is one of the network attack strategies by capturing the network traffic at the ethernet frame level and the data captured will be analysed for any sensitive information can be gathered. Semantic Scholar website says "TEMPEST (Transient Electromagnetic Pulse Emanation Standard) is an information security term that refers to the examination and control of unwanted electromagnetic energy emissions caused by electrical and electronic devices. As a result of Tempest attacks, confidential information such as state secrets, personal information such as bank passwords, and more information can be

passed on to the attackers. Unlike other known cyber-attack methods, Tempest attack methods are kept secret and those who are exposed to TEMPEST attacks are not aware of these attacks. The concept of TEMPEST is a less known cybersecurity component which can cause much greater damage if the necessary cybersecurity measures are not taken." (7)

Buffer overflow is another technique used by the cyber criminals for unauthorised access. Wikipedia explains, "a buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations." By these methodologies hackers unauthorisedly access to compromise victims' digital devices, such as computers, smartphones, tablets, and networks for malicious purposes.

DENIAL OF SERVICE ATTACKS: By sending excessive requests to the victim's computer(s), exceeding the limit that the victim's server space and making the server to crash is called Denial of service attack. The methodology generally involves by installing a Trojan on many computers, taking control of them and then making them to send numerous requests to the targeted victim computer. There is no other way except, the compromised system would need to be shut down, isolated, and cleaned. Wikipedia explains, " Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), theincoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source." Ping of Death and SYN attacks are other techniques used in DoS attack. In a Ping of death attack, the cyber criminals try to crash, freeze or strand the targeted computer or service by sending malformed or oversized packets using a simple ping command. SYN attacks uses communication protocol of the Internet, TCP/IP, to destabilize the targeted system by sending repeated SYN packets to every port on the targeted server, often using a fake IP address.

CYBER DEFAMATION: Lexology website defines "The term Cyber Defamation basically means publishing of false statement about an individual in cyberspace that can injure or demean the reputation of that individual. In India, defamation can be contemplated as both civil and criminal offence, and thus legal remedies are provided to the victims by the Indian judiciary system" (8).Cyber Defamation is an act of online attacking of any person with intent to lower the person's name and fame in the estimation of the right-thinking members of the public or to cause him to be stay awayfrom the public by exposing the person with hatred. Generally, Cyber defamation occurs when a computer connected to the internet is used as a tool, or a medium to defame a person or an entity. Cyber defamation is not different from conventional defamation except the involvement of online medium. This occurs when defamation takes place with the help of computers and / or the Internet. E.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all that person's friends. Defamation is defined under Section 499 of IndianPenal Code. In Panday Surinder Nath Sinha v. Bageshwari Prasad, the defamation guidelines were pronounced. Legal Services India website has specified that "What is actual malice- A statement made with a knowledge that it was false or with reckless disregard of whether it was false or not constitutes actual malice as explained in Sullivan's case. Also, proving the case of defamation the decision of Tsc Wai Paul v. Chang, (2001) EMLR 777 may be considered which talks about the concept of fair comment" (9).

PORNOGRAPHY: Dissemination of obscene materials, indecent exposure, child pornography and polluting through indecent exposure are coming under this category of Cyber Crime. Pornography includes the hosting of web site containing prohibited materials, use of computers for producing obscene materials, downloading obscene materials using Internet, etc. These obscene materials cause harm and corrupt the minds of adolescents. Two known Indian case laws of pornography are the DelhiBal Bharati case and the Bombay case. In the Bombay case, two Swiss couple used to force the slum children for obscene photographs. The Mumbai police have arrested the foreign nationals and tried under the Indian Laws. Online pornography is punishable in India under the Information Technology Act and Indian penal Code. Watching pornography is not illegal in India. However, production, publication and distribution of pornographic materials is illegal. Especially, child pornography is punishable up to 5 years of imprisonment and Rs.40 Lakhs fine. India Today states, "Indian laws are much stricter regarding pornography as compared to the UK laws, which allow adult consent to createand consume such content. While watching porn is not illegal in either country, the curbs are there on its creation, publication, and distribution. Any obscene material that includes children, however, is completely illegal in both countries" (10).

FINANCIAL FRAUDS: In 2021, Reserve Bank of India (RBI) has reported nearly 7400 bank fraud cases across India. Financial frauds include cheating, credit card frauds, money laundering etc. As per RBI, "Frauds have been classified as under, based mainly on the provisions of the Indian Penal Code are misappropriation and criminal breach of trust, fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property, unauthorised credit facilities extended for reward or for illegal gratification, negligence and cash shortages, cheating and forgery, irregularities in foreign exchange transactions and any other type of fraud not coming under the specific heads as above". (11). In 2019, the Cyber Crime Cell had registered 430 financial fraud cases. Number of cases rose to 1,370 in 2020 and 1600 in 2021 as of July. Cyber Crime Cells investigating these cases, suspect the involvement of organised syndicates of cyber criminals behind this steep increase of cases. Also, Covid lockdown led to huge increase in online purchases that increased the e-commerce transaction paved way for sudden surge of financial frauds.

ONLINE FRAUD AND CHEATING is one of the most lucrative businesses that are growing today inthe cyber space. Online frauds are committed with the intent to corrupt or illegally obtain another individual's personal and financial information stored online. In one recent cybercrime case, Punjab National Bank was cheated to the tune of Rs.1.39 crores through false debits and credits in computerized accounts. The internet today is used extensively for banking and commercial services. Most of the Financial transactions are taking place using internet. Though these transactions are encrypted, and only authorized persons can decrypt the message, cyber criminals use to bypass or circumvent these safeguards through fraudulent means. Generally cyber criminals target individuals who were already cheated online. Last year, the Delhi Police arrested three cyber criminals, who have created a fake

website and sent bulk messages with links to the individuals. The victims accessed the website and provided their bank details to redeem credit card points or gift cards, were cheated easily.

INTELLECTUAL PROPERTY RIGHTS CRIMES: Intellectual property right (IPR) means legal rights that protect creations and/or inventions resulting from intellectual activity in the industrial, scientific, literary, or artistic fields. Any unlawful act, by which the owner of the intellectual properties deprived completely or partially of his rights, is an offence. IPR violations include software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc. Software piracy is stealing the proprietary computer software and source code or related information. It causes heavy financial losses to the owner of the software. Copyright protects protect the creativity in the code that performs in the computer. If hardware of the computer is a body, software is the brain in that body. While hardware is a tangible property, software is considered as Intellectual property.

TROJAN ATTACK: Mondaq.com explains, "Trojan horses are code disguised as a benign program, but behave in an unexpected manner, usually a malicious manner. Trojan horses are normally injected into a foreign host while that host is browsing the Internet or downloading free utilities from the Internet. The host is normally quite unaware that a malicious program has been injected. This malicious program could hijack future HTTP sessions, monitor the activities on that host, and then relay that information back to the attacker's host and much more. Some noteworthy Trojans are ZeuS, ZeroAccess, TDSS Downloader, Alureon, Gbot, Butterfly bot, and BO2K" (12).

VIRUS ATTACK: Wikipedia states, "A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code". Virusesare malicious programs that affect the data on a computer, either by altering or deleting it. E.g., love bug virus, which affected at least 5% of the computers of the globe. The losses were accounted to be $10 million. Generally, there are two main classes of viruses. The first category consists of the file infectors, which attach themselves to ordinary program files. These usually infect arbitrary .COM and/or .EXE programs, though some can infect any program for which execution is requested, such as .SYS, .OVL, .PRG, & .MNU files. The second category is system or boot-record infectors: those viruses that infect executable code found in certain system areas on a disk, which are not ordinary files. Examples include Brain, Stoned, Empire, Azusa, and Michelangelo. Kaspersky, one of the leading Anti-malicious software producer states that "Unlike mass computer virus attacks – that aimto infect as many computers as possible – targeted attacks use a totally different approach. Instead, targeted attacks try to infect the network of a single targeted company or organisation – or apply a specially developed Trojan agent to a single server on the organisation's network infrastructure" (13).

CYBER WORMS: The term "worm" was used for the first time by science fiction author John Brunner in his book called "The Shockwave Rider". Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. Kaspersky states, "Viruses, trojans, and worms are quite possibly the most disruptive of all of the security threats" (14). Kaspersky further states. "Worms target both hard drive space and processor cycles. Worms may be working alone or in combination, can alter or delete data files and executable programs, flood e-mail servers and network connections with malicious traffic, and even create a "back door" into the systems that can allowa remote attacker to take over control of a computer entirely".

WEB JACKING: The Science Direct.com website explains "Illegally seeking control of a website by taking over a domain is known as Web Jacking" (15). Web Jacking term is derived from the term hi jacking. In this cybercrime, the hacker gains access and control over the web site and may even mutilate or change the information on the site. The motive may be for fulfilling political objectives or for financial gain. In web jacking attack method hackers compromises with the domain name system (DNS) that resolves website URL to IP address but the actual website is never touched.

ONLINE GAMBLING: There are millions of online gambling websites hosted on servers abroad. With the outbreak of the COVID-19 pandemic and the mandatory lockdown, the gambling industry has shoot up to a new high. Digital entertainment became the primary form of entertainment. Indians in mobile gaming, online gambling, and sports betting increased substantially during this period. One of the articles published in thenewsminute.com states, "Technically, in the stance of the law, gambling is illegal in the whole country of India. The laws regarding the legalization of gambling brought about complications in the Indian gambling industry. However, some states have rules that allowed gambling activities. The legalization in few Indian states has opened a new world to gambling in the territory. Hence, the future of online gambling in India is now something to evaluate and anticipate." (16). Indian Government is planning to introduce a bill to regulate online gambling in near future.

RANSOMWARE ATTACK: Ransomware is a malicious software generally introduced by the cyber criminals into victim's systems that blocks victim's access to their own data and threaten the victim todelete the data if a ransom is not paid. Proofpoint.com website states that "Ransomware attacks are alltoo common these days. Major companies in North America and Europe alike have fallen victim to it. Cybercriminals will attack any consumer, or any business and victims come from all industries. Several government agencies, including the FBI, advise against paying the ransom to keep from encouraging the ransomware cycle. Furthermore, half of the victims who pay the ransom are likely to suffer from repeat ransomware attacks, especially if it is not cleaned from the system". (17)

There are 2 types of ransomwares. They are encryptors and screen lockers. Encryptors are encryption software that encrypt data on a system and making the data useless to the victim unless a decryption key. Whereas, screen lockers, on the other hand block access with a "lock" screen, declaring the victim that the system is encrypted. Victims are notified to pay a ransom in the form of cryptocurrency to unlock the system. Once the victim paid the ransom, decryption key will be sent to the victim, but it is not guaranteed. Most of the times, victims never receive the decryption keys.

SUPPLY CHAIN ATTACK: A supply chain attack is the highly dangerous present-day trend in manycountries. In this attack, an attacker accesses a business's network via third-party vendors or suppliers' network on infrastructures like hospitals, pipelines, general utilities, electrical supply, HVAC plants, and water supply centres and bring down temporarily or even permanently.

ILLEGAL TRAFFICING: Illegal trafficking using computers as a tool in drugs, human beings, arms weapons etc are coming under the category. This would include sale of narcotics, weapons, and wildlife etc. The criminals use pseudonyms to conceal their identity. Recently a drug racket was busted in Chennai where drugs were being sold under the pseudonym of honey. The modus operandi generally includes by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

CARD DATA THEFT: Cards are very essential instrument for financial transaction. These cards are containing machine-readable magnetic code, allowing the holder to make transactions. Cards are designed to follow ISO 7810 standard to ensure uniformity and read reliability worldwide. Cyber criminals commit many types of crimes in this regime. Cyber criminals use different modalities to steal card data and commit variety of frauds like Card Trapping, Counterfeit Fraud, Merchant Fraud, Card-not-present Fraud, Lost or Stolen Cards, Mail non-receipt Fraud, Fake Website Fraud, Identity Theft, Application Fraud, Account Take-over Fraud, Card Brokering frauds are the most prevalent card frauds.

CYBER ACTIVISM: Technopedia describes, "Cyberactivism is the process of using Internet-based socializing and communication techniques to create, operate and manage activism of any type. It allows any individual or organization to utilize social networks and other online technologies to reach and gather followers, broadcast messages, and progress a cause or movement. Cyberactivism is also known as Internet activism, online activism, digital activism, online organizing, electronic advocacy, e-campaigning and e-activism" (18). Cyberactivism uses social networking portals and platforms to share and broadcast illegal messages to the public. These online portals include Twitter, Facebook, LinkedIn, YouTube, and other social networks. Email, instant messaging (IM) and other online tools are forming part of this communication. These cyber criminals are part of e-activists, who uses the online communication for various purposes

PANDEMIC RELATED PHISHING: Phishing is one of the common techniques for cybercriminalsto steal confidential and personal data like debit/credit card details, login credentials, email id and many more. Hackers act as authentic and trusted entities with valid promises to instigate victims to follow their orders. Due to the ongoing pandemic and the need for vaccination, these cybercriminals have started vaccine-related phishing to innocent victims. This has become one of the top emerging cybercrime trends in 2021. Instigating victims to provide access to personal information through emails and calls with a promise to provide vaccine in the nearby future or email links to learn about health advice, precautions, or change in work-from-home policies.

3. FUTURE TRENDS OF CYBERCRIMES

The coronavirus pandemic has forced the world to work from home and shift to the digital model withsupport from the trend of digital transformation through smart devices and internet connections. Cybercriminals utilising the situation have shown their capabilities from organising identity theft on social media to infiltrate organizations and hold their data for ransom. There are innovative creative ways for cyberattacks on companies to steal confidential data efficiently without getting noticed. Data breach in cybercrimes happens when cybercriminals bypass outdated cybersecurity measures of a company. Emerging cybercrime trends include Data Exfiltration, Blend of AI and IoT with 5G attacks, Cloud attacks, Cryptojacking, Malware trends, Cyber Activism and Supply Chain Attack.

DATA EXFILTRATION: Data exfiltration is a technique used by cyber criminals to extract sensitive data of the target organization. Cyber criminals generally use social engineering and phishing attacks to gain access into victims database to copy and transfer sensitive data. Data exfiltration occurs in twoways, through outsider attacks and via insider threats. Both are dangerous threat sources. Fortinet.comspecifies, "the techniques cyber criminals use to exfiltrate data from organizations' networks and systems are becoming increasingly sophisticated, which help them avoid detection. These include anonymizing connections to servers, Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS) tunnelling, direct Internet Protocol (IP) addresses, fileless attacks, and remote code execution" (19). The Common targets include financial records, customer information, and intellectual property/trade secrets. After the data exfiltration, the stolen data is used to blackmail the organization for ransom. Preventing data from being exfiltrated includes 1. Blocking unauthorized communication channels, 2. Credential theft and phishing prevention, 3. Using tools that can detect legitimate application and communication activity and 4. User education.

ARTIFICIAL INTELLIGENCE & IOT DEVICES: An article on The future of drones & robots published in the Analytics Insight Website indicates, " The future of farming will be unmanned tractors controlled via GPS; drones that kill vermin in the fields from above; and highly efficient bull sperm used to produce genetically optimized calves. Tech analysts IDC predict there will be 41.6 billion connected IoT devices worldwide by 2025" (20). The blend of AI and IoT devices with the 5G network has promised to ease the life of society through smart devices in smart homes. But this is a call for cybercriminals to get attracted and steal more data possible. There is no guarantee that these devices can fully protect from a data breach in cybercrimes. AI can prevent criminal activities in acity but when any device is connected to the Internet, it is a hack-prone zone. IoT is usually associatedwith cloud-based servers and don't have operating systems. That doesn't mean that they are free from cyber-attacks. Cyber-attacks on IoT devices can compromise the functionality and misuse of devices. Sensitive data can also be stolen from these devices.

CYBER ATTACKS ON CLOUD PLATFORMS: Companies have started adopting Cloud-based computing systems to store sufficient data, provide access to software applications and offer efficient services through the Internet. But cybercriminals have identified this new space to become a target ofa data breach in cybercrimes. There are many ways to attack cloud computing

services, and hackers are constantly working on developing more sophisticated methods. An article published in Dzone.com describes, "By the year 2025, the cloud computing market is expected to grow $832.1 billion. Trend Micro predicts that code injection attacks can be utilized to attack cloud platforms. These attacks can be carried out through third-party libraries, from SQL injection and cross-site scripting. Attackers inject malicious code through third-party libraries and ensure that the code is downloaded and executed by individuals unintentionally" (21). National Institute of Standards and Technology (NIST)and many other Institutions like ISACA, SANS have developed cloud computing standards to secure cloud environment from cyber criminals. However, it is predicted there will be a lot of new tools that can exploit by penetrating cloud computing and cyber criminals are working on the loopholes in the present control environment.

CRYPTOJACKING: As cryptocurrency becomes popular, a rise in crypto-specific cyberattacks is inevitable. Cryptocurrency is managed by a decentralized using encrypted blockchain technology rather than by a centralized agency like Reserve Bank of India. As the digitalized transactions are processed through Blockchain Distributed Ledger Technologies, these transactions could be manipulated by cyber criminals easily for malicious purposes. One of such criminal activity is called Cryptojacking. The Interpol defines, "Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. This usually occurs when the victim unwittingly installs a programme with malicious scripts which allow the cybercriminal to access their computer or other Internet-connected device, for example by clicking on an unknown link in an e-mail or visiting an infected website. Programmes called 'coin miners' are then used by the criminal to create, or 'mine', cryptocurrencies" (22). Cyber criminals will use this technique for their consistent income, as there is no regulatory authority to oversee these digital transactions.

MOBILE MALWARE ATTACKS: Mobile smart devices become an essential part of human life. As people become more dependent on their mobile devices, this creates a very lucrative target for cybercriminals. Smart phone cyber-attacks are increasing day by day, particularly on the Android platform as the user base has grown exponentially. Mobile smart device users are going to be targeted by the cyber criminals mainly on finance related applications, such as mobile banking. Many unknown software developers are developing sophisticated mobile malware without knowing the fact that this software is going to destroy the mobile platform in near future. At the same time, organizations assisted by ethical hackers are preparing to combat the situation by detecting and preventing malware in mobile devices and planning for a comprehensive and multi-level approaches. The Enigma Software says, "New methods and variants continue to be implemented, allowing these lesser-known and uncommon malware packages to keep their attacks going for a longer period oftime, even if this means blatantly attacking the people who are trying to study them. There have been many new and improved attacks discovered in recent reports" (23).

STATE SPONSORED CYBER TERRORISM: Cyberspace is a lawless land. Cyber warfare using this online cyberspace will be the next dangerous endemic, especially applies to state-backed cyber- warfare. Cyber terrorism is defined as "the premeditated use of disruptive activities, or the threat thereof, in cyberspace, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives". Cyberterrorism can also be described as politically motivated attacks in cyberspace. One such incident we come across that a Chinese Government sponsored group of cybercriminals have caused a power outage- in Mumbai on October 13, 2020, shows the starting point of state sponsored cyber sabotage. The Science Direct magazine states, "'Cyberterrorism entails leveraging ICT infrastructure to create real-life damage or critical disruption with the goal of promoting the attackers' underlying political, religious, or social issue. Terrorists may force their intentions into the digital space to advance their agendas"(24). Cyber Terrorism tools include Denial of Service (Dos) attacks and Distributed Denial of Service attacks (DDoS), web defacement, misinformation campaigns, unauthorized access to sensitive information with the goal of corrupting, stealing, or destroying the data, exploitation of systemvulnerabilities and malware attacks.

4. CONCLUSION

Cyber experts predict $5 trillion worth losses to organizations in 2024 in the form of fines and penalties for the data breaches alone. Future cybercrimes not only going to affect the individuals and organizations, but also going to destabilize the Governments and International cooperation. Cyber specialists recommend, anticipatory compliance and predictive threat analysis approach can save the world from future cyber-attacks. The best way to move forward is to secure our future by taking everyprecaution possible, keeping in mind the current cyber climate, and predicting future conditions.

5. REFERENCES

[1] Phishing Statistics (Updated 2021) - 50+ Important Phishing Stats - Tessian
[2] Nearly 2,000 malicious COVID-19-themed domains created every day - TechRepublic
[3] https://www.windstream.com/Support/Internet-Security/Internet-Support/Different-types-of- threats-on-the-Internet.
[4] https://www.kapurthalapolice.gov.in/cyber-crimes.
[5] https://www.kaspersky.co.in/resource-center/threats/how-to-avoid-cyberstalking
[6] https://www.marshall.edu/wcenter/stalking/cyberstalking/
[7] https://www.semanticscholar.org/paper/TEMPEST-Attacks-and-Cybersecurity-Aydin/fbbdf168ba7888688f83e5f55ace018b89731322https://blog.ipleaders.in/cyber-defamation-india-issues/
[8] https://www.lexology.com/library/detail.aspx?g=d3075f4d-afb5-4920-bf59-26cf5d054ab8
[9] https://www.legalserviceindia.com/article/l380-Online-Defamation.html

[10] https://www.indiatoday.in/india/story/explained-indian-and-uk-laws-on-pornography
[11] https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=578
[12] https://www.mondaq.com/india/patent/830332/ip-protection-of-software-in-india-8208- patent-or-copyright
[13] https://www.kaspersky.co.in/resource-center/threats/targeted-virus-attacks
[14] https://www.sciencedirect.com/topics/computer-science/trojan-horse
[15] https://www.geeksforgeeks.org/web-jacking/
[16] https://www.thenewsminute.com/article/future-online-gambling-india-155640
[17] https://www.proofpoint.com/us/threat-reference/ransomware
[18] https://www.techopedia.com/definition/27973/cyberactivism
[19] https://www.fortinet.com/resources/cyberglossary/data-exfiltration
[20] https://www.analyticsinsight.net/apocalypse-or-opportunity-reimaging-the-future-of-drones- robots/
[21] https://dzone.com/articles/top-5-evolving-cybersecurity-threats-to-cloud-comp
[22] https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking
[23] https://www.enigmasoftware.com/the-future-of-malware-beware-of-new-trends-and-attacks/
[24] https://www.sciencedirect.com/topics/computer-science/cyber-terrorism

