Artificial Intelligence in the Digital Age: A Tool for Cyber Terrorism and a Sword for Cyber Security

Dr. Dipankar Debnath[1]
Dr. Sanjay Dutta[2]

Abstract

Artificial intelligence (AI) is a new frontier in the field of technology. In the emerging technological inventions AI played a pivotal role unfurling new arena of development world has ever been experienced. It has a multi-disciplinary approach. Where on the one hand, it has been using to find every possible solution for the problems mankind has been facing in the fields be it social, economic, political etc. On the other, it has invited unwanted consequences of risk in the digital world. In the social field, AI, apart from contributing to health, education, transport, service industries, consumer products, agriculture etc. it has started creating its dominance in the cyber world as well. Cyber world, a virtual world on which people's dependency is increasingly growing without knowing its far reaching impact has been attracted the attention to the world community only during the recent past. The proliferation of internet alongwith computer and smartphone which are user friendly made it indispensable for us. Consequently, its misuse has opened vistas of risk involve in it. The increasing incidents of cyber-crimes including cyber terrorism using AI mechanisms has become a cause of concern to the world community making it indispensable to explore strong security measures to fight against such evil. It's a challenge to the whole world. Taking into consideration the beneficial as well as the ill effect of the application of AI an attempt has been made in this article to understand how AI has been contributing as a shield and a sword and what measures could be possible to be adopted to make the cyber world more secured.

Keywords: *Artificial Intelligence, Cyber Crime, Cyber Terrorism, Cyber Security, Generative AI.*

---

[1] Assistant Professor, Department of Law, University of North Bengal, West Bengal, India.

[2] Assistant Professor, Department of Law, University of North Bengal, West Bengal, India.

I. Introduction

Human being has been considering as the most intelligent specieson earth successfully able to penetrate through each and every field to which a minimum of curiosity exists or remains undiscovered. It has succeeded to intrude to whatever exist on the earth and beyond whether reaching to Mars or Moon or even to Sun to the deep into the Black Hole. Applying its super intellect capacity, human beings made every mission successful exploring the possibility of what could be beneficial for their mere survival peaceably and without any harmful effect. For thousands of years, depending on and applying our intellect, we have been able to conclude as to how a mere handful of matter could be perceived, understood, predicted, and manipulated in order to fulfil desires.

In the field of technology also our experts are able to reach to many areas exploring and contributing to vast field of possibilities and opportunities. One of such field being the invention of Artificial Intelligence (AI) during the recent past that is built on intelligent entities and not just to understand it. It is one of the newest fields in science and engineering. As it has opened a new vista of opportunities meeting the needs of the people in general, however, it in turn posed a serious threat to the mankind to which there is an urgent need to address to. For example, the application of AI as a tool for cyber terrorism as well as to combat the same, has been a great challenge to the experts who have been constantly making every possible opportunity to do away with the evil with a view to create a world which is free from all the harmful effects of technological invention. Unfortunately, while approaching towards this it has to counter and overcome with the obstacles created by those who have been constantly making all efforts manipulating the cyber world for their unlawful gains. The negative impact of the application of AI therefore, cannot be ignored as according to Newton's third law-for every action in nature there is an equal and opposite reaction. These technologies can also be manipulated for malicious ends when they fall into the wrong hands. Exploitation of AI for

terrorist to contribute to the comprehension of the potential threat posed by the utilisation of AI by terrorist groups[3] has become a matter of great concern.[4]

II. Artificial Intelligence: Today's Dark Horse

AI is all about thinking humanly, acting humanly, thinking rationally and acting rationally as observed by Stuart Russel and Peter Norvig.[5] John McCarthy is said to be the first person to coined the term in 1956. Although there is no internationally accepted definition of the term, according to Richard A Roehrl, AI is a kind of software technology with at least one of the following capabilities,[6] perception, decision making, prediction, automatic knowledge extraction and pattern recognition from data, interactive communication etc. This view encompasses a large variety of subfields, including machine learning.

According to Marie Francisco, AI "refers to a class of computer programs designed to solve problems requiring inferential reasoning, decision-making based on incomplete or uncertain information, classification, optimisation, and perception."[7]

According to the World Economic Forum Report, Harnessing Artificial Intelligence for Earth, AI refers to computer systems that "can sense their

[3] D.C.Verma, S.S.Gartner, D.H.Felmlee, D. Braines., & R. Yarlagadda, *Using AI/ML to predict perpetrators for terrorist incidents. Proceedings of SPIE,* THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING, (2020), https://doi.org/10.1117/12.2558804

[4] E.Ismayil, & E. K. Ismayil, *Media and Terrorism in the 21st Century,* MEDIA AND TERRORISM IN THE 21st CENTURY, (2022), https://doi.org/10.4018/978- 1-7998-9755-2

[5]The Role of Artificial Intelligence in Achieving the Sustainable Development Goals, Nature Communication(2020),https://doi.org/10.1038/s41467-019-14108-y www.nature.com/naturecommunications.

[6] Richard A Roehrl, Beyond a Black-Box Approach to Artificial Intelligence Policy-A Simple Guide to Definition, functions and Technology Types, Science-Policy Brief for the Multistakeholder Forum on Science, Technology and Innovation for the SDGs, May 2022, United Nations, https://sdgs.un.org/

[7] Marie Francisco, Artificial Intelligence for Environmental Security: National, International, Human and Ecological Perspectives Elsevier, Vol. 16, Science Direct, April, 2023, www.sciencedirect.com.

environment, think, learn, and act in response to what they sense and their programmed objectives,"[8]

The Britannica on-line Dictionary[9] defines AI as the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.

The Cambridge English Dictionary[10] defines the term as: the use or study of computer systems or machines that have some of the qualities that human brain has, such as the ability to interpre and produce language in a way that seems human, recognise or create images, solve problems, and learn from data supplied to them.

AI therefore, encompasses a range of technologies designed to simulate human intelligence, including machine learning, natural language processing, and computer vision. As AI applications become prevalent in sectors such as healthcare, finance, and education, studying their social impacts is becoming increasingly important. AI is not just a technological innovation; it is a phenomenon that affects economic, social, and cultural dynamics[11].

III. Cyber Crimes Vis-A-Vis Cyber Terrorisms

Terrorism is a consistent phenomenon world has been encountering since time immemorial in different shapes and forms. However, the contemporary world has witnessed significant changes in the nature of terrorism. The conventional acts of terrorism have gradually changed to a new direction with the proliferation of internet i.e. cyber world which has been considering more

[8] Renee Cho, Artificial Intelligence-A game Changer for Climate Change and the Environment, Climate,Ecology, Columbia Climate School, June 5, 2018, http://news.climate.columbia.edu/2018/06/05artificial-intelligence-climate-environment/.

[9] Britannica, https://www.britannica.com/technology/artificial-intelligence.

[10] Cambridge On-line Dictionary, https://dictionary.cambridge.org/dictionary/english/artificial-intelligence.

[11] Aytul Ercil, Impact of Artificial Intelligence Applications on Society, AI Horizon Journal of AI Ethics & Integrity International Association, https://ai-ei.org/impact-of-artificial-intelligence-applications-on-society/?gad_source=1&gad_campaignid=22979320730&gbraid=0AAAAA_P7btrMtUrAGQ1ENGwB-SA1g8VlO&gclid

destructive and deadlier in nature. The invention and development of internet make it possible for people to communicate with the world sitting at home, be it personal or commercial. The more the dependency, the heavier is the risk of vulnerability involve in it despite making and adapting all sorts of security measures. This is obvious because to ensure a secured measure is a misnomer because the more securely it would be protected the more target it will be. The terrorists with their knowledge and expertise are successful in developing the noxious combination of weapons and information technology. Cyber world has become a tool for the terrorist's activities which involves recruitment, training, planning, resource and data transfer, and intelligence sharing between and among the terrorist groups. All these leads to cyber terrorism which is a subset of cyber-crime. Cyber-crime is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology. The oxford Dictionary defined the term cyber-crime as "Criminal activities carried out by means of computers or the Internet"[12].

Cybercrimes can be classified broadly into four different categories like –

1. cyber-trespass (unauthorised digital access);
2. . cyber-deception/theft (online fraud, identity theft etc.);
3. cyber-obscenity (circulation of sexual exploitation materials) and
4. cyber-terrorism.[13]

Though all of the abovementioned cybercrimes are a big threat to any society and must be prevented at all costs, cyber-terrorism most recently has been a pressing concern for all the developed countries and the worst part being that there aren't many systematic structures to identify, monitor and prevent such crimes[14]. As this crime is committed by a perpetrator using the special knowledge of the digital space that is referred to as a 'cybercrime'[15].

---

[12] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 4th January, 2016)

[13] Adam M. Bossler & Tamar Berenblum, *Introduction: new directions in cybercrime research*, 42(5) JOURNAL OF CRIME AND JUSTICE 495, 495 (2019).

[14] Arindam Bhardwaj, The Dark Web and Cyber Terrorism: The Urgent Need of Actions Against Trade in Illicit Goods,

Cyber Terrorism is of recent vintage and was coined by computer whiz Barry C. Collin. A widely acceptable definition of cyber terrorism is "a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda".[16]

According to the U.S. Federal Bureau of Investigation, "Cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents"[17].

As per Section 66F of the Information Technology Act, 2000, cyber terrorism involves using digital tools to threaten national security, sovereignty, and public safety. Key categories include critical infrastructure attacks, hacking government databases, cyber-espionage, spreading malware/ransomware, and disrupting vital services often originating from cross-border state-sponsored actors[18]. Common forms of cyber terrorism include infrastructure sabotage, massive DDoS attacks, data theft or manipulation, disruption of essential services and psychological propaganda disrupting essential services and threaten national security. The attacks on Ukrainian infrastructure in 2024-25, major coordinated cyber-attacks involving 19 hours of DDoS attacks on the President of India's website, Russian-linked hacking of Baltic state government portals etc. are examples of cyber terrorism incident which attracted the attention to the world community showing rising concern of such areas of terrorism.

---

efaidnbmnnnibpcajpcglclefindmkaj/https://iica.nic.in/images/FOIRNews/The-Dark-Web-Cyber-Terrorism-Arindam.pdf

[15] Adam M. Bossler & Tamar Berenblum, *Introduction: new directions in cybercrime research*, 42(5) JOURNAL OF CRIME AND JUSTICE 495, 495 (2019).

[16] Amaresh Pujari, Cyber Terrorism: World Wide Weaponisation, TN Police Sesquicentennial Anniversary Souvenir, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf

[17] *Ibid*.

[18] Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi

IV. Indian Cyber Attack Statistics 2026[19]

Weekly attacks — Education sector	7,684 per org/week	Check Point 2026
Weekly attacks — Government sector	4,912 per org/week	Check Point 2026
Weekly attacks — Business Services	3,747 per org/week	Check Point 2026
Total malware detections (Oct 2024–Sep 2025)	265.52 million	Seqrite India Report 2026
Malware detections per minute	505 per minute	Seqrite 2026
Trojans & file infectors share	70% of all malware	Seqrite 2026
SIM cards blocked for cyber fraud	9.42 lakh	CERT-In / DoT
India cybersecurity budget (2025–26)	₹782 crore	Union Budget
India's share of global endpoint malware	12.4%	Acronis 2025
Ransomware extortion victims increase	+53% globally in 2025	Check Point 2026
Ransomware surge in Jan 2026	+31.4% above prior avg	Cyble, Feb 2026
Cloud environments share of detections	62% of all detections	DSCI telemetry
India WEF national cyber risk ranking 2026	#1 national risk	WEF Global Risk Report 2026

Cyber terrorism may affect a country's reputation and stability, financial losses occur, and in some cases, even lives can be lost. As a result of cyber-attacks, critical infrastructure, such as power grids, hospitals, and transportation systems, can also be disrupted, leading to widespread disruptions and distress. Most of the time, cyber terrorism can result in death or physical harm, an explosion, a plane accident, water pollution, or a major economic or political

[19] Jay Thakkar, Recent Cyber Attacks in India 2025-2026, https://eventussecurity.com/cybersecurity/india/cyber-attacks/

loss. If it has a large effect, cyber terrorism may be conducted against essential infrastructure[20].

Forms of cyber terrorism.

A. Privacy violation.

B. Secret Information appropriation and data theft.

C. Demolition of e-governance base.

D. Distributed denial of services attack.

E. Network damage and disruptions.

V. Cyber Terrorism: Role of AI as Perpetrator

According to a 2021 UN report, 44 percent of experts surveyed believed the malicious use of AI by terrorists was very likely, and 56 percent believed it was somewhat likely. No expert surveyed believed it was unlikely[21].

In the last few years, artificial intelligence (AI) has taken centre stage in public, academic, and political discussions. Groups such as Al-Qaeda, ISIS and Hizbollah etc. are using such technology to achieve their respective goals disrupting the stability of their targetted countries. Therefore, it is important to put serious attention on it as to how terrorists are using AI-based technologies to meet the end. For example, using synthetic (fake) images, videos, or audio that align with the organisations' values could help increase the breadth of propaganda produced, intensify messages, and affect people's attitudes and emotions[22]. In the Gaza war the terrorists had used generative AI (a subsets of AI) as different images have been leaked on the internet to instigate more violence and increase their propaganda of disinformation. Further, the images and videos of the Israrael Defence Forces soldiers wearing diapers on social

[20] Saman Iftikhar, Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures, (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10803091/

[21] UN Office of Counter-Terrorism and UN Interregional Crime and Justice Research Institute, Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes (UN Office of Counter-Terrorism and UN Interregional Crime and Justice Research Institute, 2021), 11.

[22] Clarisa Nelu, Exploitation of Generative AI by Terrorist Groups, (June, 2024), https://icct.nl/publication/exploitation-generative-ai-terrorist-groups

media appeared to be generated by a Hamas-affiliated group using generative AI, and it aimed to undermine the Israeli army.

Terrorists may utilise AI for cyber-terror purposes to automate their attacks, utilising machine learning to exploit cybersecurity weaknesses. By applying machine learning, hackers can develop algorithms that are more complex and accurate; every time a hacker attempts to enter a system and fails, through a method of self-learning and automation, the next cyber-attack would be more lethal. This gives cyber terrorists incredible potential in the amount of damage they could do[23]. The use of autonomous AI driven weapons or drones to carry out attacks with minimal human intervention by the groups could target individuals, infrastructure, or entire populations posing serious secrurity threats for defense and law enforcement agencies of the government.

The use of neural networks by the terrorist groups with an intention to collapse government controlled power grids and transportation systems may thereby create widespread chaos. In addition to it, accessing government confidential data stored and maintained in the secured electronic systems, the terrorists use prompt injections to disrupt security agencies' use of generative AI to respond to the growing crisis. As AI technologies become ubiquitous in modern life, while making societies more prosperous they can also make them more vulnerable in the hand of the terrorist groups or agencies. The exploitation of AI by these groups to execute their operations while exploiting the public and private use of AI to their own ends is a challenge which is needed to urgently address to by the government appointed experts.

Further groups like Da'esh utilised automated 'bots', software applications that execute automated tasks on the internet that mimic human behavior at high speeds and large scales to amplify their messages on social media, increase visibility, and engage with potential recruits.[24] Spreading misinformation and

[23] Mateja Nickolic, Artificial Intelligence: Terrorism and International Relations, (April, 2024), Centre for International Relations and Sustainable Development, https://cirsd.org/opinions/artificial-intelligence-terrorism-and-international-relations/

[24] Abdullah Alrhmoun et al., *Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem,* TERRORISM AND POLITICAL VIOLENCE 36, no. 4 (2024): 411; and "What Is a Bot? 5 Common Bot Attacks: Detection &

fake news through social media platforms and online forums to sow discord, amplify grievances, and recruit sympathisers with the help of AI is another methods that may also disrupt the governnent to focus on its own activities. AI-powered bots and algorithms amplify the reach and impact of these disinformation campaigns, making it challenging to discern truth from fiction. Likewise, AI enable crypto trading bots have been reported in fundraising operations. The Financial Action Task Force (FATF) and other financial watchdogs flagged suspected terror funding through AI-enabled automation[25]. Utilising AI-powered surveillance technologies, terrorist groups gather intelligence on potential targets, monitor security measures, and evade detection by law enforcement agencies. They may use facial recognition, pattern recognition, or natural language processing algorithms to analyse vast amounts of data and identify vulnerabilities or opportunities for attack[26]. Similarly, terrorist organisations are becoming more adaptive, leveraging AI to refine their strategies and increase operational efficiency, including using AI for reconnaissance, targeting, and optimising logistics.[27]

Large Language Models (LLMs)[28] are being developed to speed the coding and scaling of cyberattacks, though destructive cyberweapons appear limited.

Management Options," HUMAN Security, n.d., accessed Oct. 22, 2024, https://www.humansecurity.com/learn/topics/what-is-a-bot, accessed Oct. 22, 2024.

[25] Soumya Awasthi, Jihadi Use of Artificial Intelligence: A Growing Threat in the Digital Age, Observer Researche Foundation, https://www.orfonline.org/expert-speak/jihadi-use-of-artificial-intelligence-a-growing-threat-in-the-digital-age

[26] K. Krisnayonto, S. Suryadi, *Exploring the Dark Horizon: Artificial Intelligence (AI) as Cyber Terrorism Tools,* JOURNAL OF TERRORISM STUDIES, Article 1, Vol. 7, (2025), https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?params=/context/jts/article/1111/&path_info=auto_convert.pdf

[27] C. Anthony Pfaff, The Weaponisation of Artificial Intelligence the Next Step of Terrorism and Warfare, Centre of Excellence Defence Against Terrorism (COE-DAT), efaidnbmnnnibpcajpcglclefindmkaj/https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf

[28] LLMare a subset of generative AI that use natural language processing "to understand and generate human-like language outputs."60 They are trained on a wide variety of data and are "strictly used for language and text related tasks," or text and image-generation capabilities61 ChatGPT and other LLMs cannot produce new content on their own: they are limited by the data on which they are trained.

Hacking groups from China, Iran, North Korea, and Russia have used LLMs for computer-code generation. For example, the Chinese hacking group Chromium used LLMs to generate scripts and automate complex cyberoperations, and the Chinese hacking group Sodium attempted to use LLMs to produce malicious code[29].

VI. Cyber Terrorism in India

India is in the midst of one of the most ambitious digital transformations ever attempted by a nation. The evolution of cyber terrorism in India reflects the erosion of boundaries between cyber warfare, information operations, and psychological influence. China-linked RedEcho has been constantly making all sorts of efforts penetrating India's power and port sectors through ShadowPad. Similarly, APT36 as conducted persistent espionage against governments defence, academic and diplomatice targets using CapraRAT, ElizaRAT multi-platform payloads etc.

Both illustrate the weaponisation of cyberspace for intelligence gathering and potential disruption of national infrastructure. Despite institutional advances through CERT-In, NCIIPC, and the Defence Cyber Agency, India's cyber-intelligence ecosystem continues to face constraints in real-time data fusion, predictive analytics, and inter-agency coordination[30].

The financial sector of India also faces significant cyber threats which cause severe monetary damage while damaging confidence in the public. Metropolitan Business Research Centre data reveals terrorists use advanced strategies to penetrate banking security defences thus causing serious financial losses, and reputational harm. Additionally, terrorists in India used PayPal and Amazon to channel funds and procure materials for attacks, including components for the Pulwama bombing[31]. Thus a comprehensive AI-enbled defense approach is essential for the region's stability. Keeping in mind the

[29] Elias Groll, "State-Backed Hackers Are Experimenting with OpenAI Models," CyberScoop (website), February 14, 2024, https://cyberscoop.com/openai-microsoft-apt-llm/.

[30] CLAWS JOURNAL l Vol. 18, No. 2. Winter 202548 sujeet PIllaI, julfIkar and kunal koregaonka

[31] Times of India, July 9, 2025, https://timesofindia.indiatimes.com/india/component-of-pulwama-ied-was-ordered-via-amazon-fatf/articleshow/122328457.cms

current geo political scenario and the rise of India in world politics, AI will be the key enabler which will help India rise in the World order securing the cyber space for itself and the world at large.

VII. Cyber Security

In the era of digital world cybersecurity becomes indispensable. The field covers all the processes and mechanisms by which computer-based equipment, information and

services are protected from unintended or unauthorized access, change or destruction. Cybersecurity is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. Cyber Security is a subset of information security which deals with securing the information, data from both internal and external cyber threats. It is a proactive practice to safeguard the confidential information of the organization from unauthorized access by enforcing the layered security policies and protocol.

The cyber security provide protection to all the stakeholders within the realm of an organisation, employees, and government who have been facing critical challenges while using the technological devices in a digital world. Various sensitive data which includes personal information, health information as well as government and industry information of various kinds nowadays expose to vulnerability as the information may at any point of time targeted by the hackers to be exposed in order to fulfil their needs. The increasing number of cyber threat, regulation and compliance requirements, education, training and employment opportunities therefore, making it inevitable to protect online environment with the help of a medium called cyber security.

According to Section 2 (nb) of the Information Technology Act, 2000 cybersecurity means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. Although the definition is not comprehensive, however this definition provides us with the critical areas where the term cybersecurity is applied. A formal definition of cybersecurity provided by Merriam-Webster dictionary as measures taken to protect a computer or computer system (as on the Internet) against unauthorised access or attack.

The cybersecurity landscape in India has witnessed an unprecedented evolution throughout 2024, marked by both escalating threats and significant advances in detection capabilities. As cyber threats become more complex and pervasive, the role of governments in ensuring cybersecurity has become more critical. By 2025, many nations will have enacted stricter cybersecurity regulations to protect businesses and citizens from cybercrime. With 971 million internet subscribers, India's digital landscape is growing rapidly[32] marking a 28% increase as revealed by Telecom Regulatory Authority of India (TRAI). Between 2019 and 2023, cyber-attacks on the Indian government increased by 138 percent. The Reserve Bank of India reported that data breaches cost India $2.18 million in 2023, a 28 percent increase in three years[33]. According to the latest data, in 9.4% of Indian homes, there is a computer. The Union Budget 2025-2026 allocated ₹782 crore for cybersecurity projects[34].

The surge in cybersecurity incidents from 10.29 lakh in 2022 to 22.68 lakh in 2024 reflects the growing scale and complexity of digital threats in India. At the same time, the financial toll is becoming more pronounced, with cyber frauds amounting to ₹36.45 lakh reported on the National Cyber Crime Reporting Portal (NCRP) as of 28 February 2025. While the numbers point to increasing challenges, they also highlight remarkable progress in the nation's detection and reporting mechanisms[35].

---

[32] FE Tech Desk, India's Internet Subscribers Cross 971 Million Mark Amid Decline in Telephone Users: TRAI Reveals, (Jan. 2025), https://www.financialexpress.com/life/technology-indias-internet-subscribers-cross-971-million-mark-amid-decline-in-telephone-users-trai-reveals-3705641/

[33] *Ibid*.

[34] Curbing Cyber Frauds in Digital India, Min. of Info. and Broadcasting, Govt. Of India, (Oct, 2025) https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3&reg=3&lang=2

[35] Curving Cyber Frauds in Digital India, Backgrounders, Press Information Bureau, Govt. of India, efaidnbmnnnibpcajpcglclefindmkaj/https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/oct/doc2025108660701.pdf

A. Types of Cybersecurity

Information Security: It is a measure adopted in order to secure sensitive data, such as personally identifiable information (PII) and data stored in databases and files from hackers and cyber criminals. It refers to the tools and processes for preventing, detecting and remediating threats to sensitive information, whether digitised or not. It prevents theft of data and also the condition where hackers extort ransom from users for their sensitive information. It covers security measures such as regular backups, encryption of data, both in transit and at rest, and access controls including multifactor authentication. It basically includes User authorisation, authentication and cryptography.

Network Security: Deals with protecting the integrity, confidentiality and safety of the network components such as communication infrastructure (devices, hardware, software etc.) used by the users and also avoiding denial of service attacks where the original and legitimate cannot be able to use that computer network. Network security solutions ae designed to identify and block various cyber attacks. It includes services like firewalls, antivirus software, Data Loss Prevention (DLP), Identity Access Management (IAM) and Virtual Private Networks. In addition to this advanced and multi-layered threat prevention technologies include Intrusion Prevention System (IPS), Next-Gen Antivirus (NGAV), Sandboxing and Content Disarm and Reconstruction (CDR).

Application Security: Application security refers to the technologies, policies and procedures at the application level that prevent cybercriminals from exploiting application vulnerabilities. It involves a combination of mitigation strategies during application development and after deployment. Web applications that are directly connected to the Internet, are targets for threat actors. It involves checking code testing and review, point frequency security testing, and ensuring that no applications have security flaws or vulnerabilities that may be exploited for example cross-site scripting and broken authentications. With application security, the OWASP Top 10 attacks can be stopped. It also prevents bot attacks and stops any malicious interaction with applications and APIs.

Cloud Security[36]: It refers to cyber security solutions, policies, services, administrative, and technical controls that protect an organisations's entire cloud deployment and its components like infrastructure and data from attacks. It ensures sensitive information is safe from data breaches and other vulnerabilities, whether stored in public, private or hybrid clouds.

As businesses continue migrating to the cloud, ensuring the security of cloud infrastructures is more important than ever. One of the cloud computing's biggest security challenges is providing users with safe, frictionless access to their most essential applications. Singularity Cloud Security provides proactive security for cloud environments, safeguarding both cloud-hosted applications and the data they manage. Organisations often mitigate security risks using identity and access management (IAM), a key strategy that ensures only authorised users can access specific resources. IAN solutions are also integral part of network security.

Endpoint Security: It focuses on protecting the devices that serve as access points to an organisation's network. This includes servers, mobile devices, laptops and desktops etc. The securing of these devices, as well as the data they carry, is regarded as endpoint security. These devices or endpoints, expand the attack surface, providing potential entry points for cybercriminals to exploit vulnerabilities and infiltrate the broader infrastructure. Advanced threat prevention software includes anti-ransomware, anti-phishing protocols, as well as endpoint detection and response solutions to ensure that these end-user devices stay secure[37].

Zero Trust: It is modern cybersecurity model that assumes no user or system, whether inside or outside the network, is automatically trustworthy by default. The traditional perimeter-focused way of building walls around the most important systems and assets of a company can be breached by insider threats, as well as by the dissolution of that perimeter. However, this approach as several issues, such as potential for insider threats and the rapid dissolution of the network perimeter. Moreover, with the evergrowing trend toward cloud

[36] Types of Cyber Security: Safeguarding your Business, https://www.sentinelone.com/cybersecurity-101/cybersecurity/types-of-cyber-security/

[37]What is Cyber Security, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

computing and moving away its assets off premises, what is needed is stronger security than perimeter-focused can offer. Zero trust security is the answer.

Internet of Things (IoT) Security: While IoT devices certainly delivers productivity benefits however, it also exposes organisations to cyber threats at the same time. IoT Security reduces the vulnerabilities of wearable smartphones, and all connected devices found in smart homes. These devices are protected with discovery and classification of the connected devices, auto segmentation to control network activities and using IPS as a virtual patch to prevent exploits against vulnerable IoT devices. IoT security also incorporates secure communication protocols as well as access control mechanisms. It scans vulnerabilites and will keep updating and patching the software.

Operational Security: This security uses same solutions and techniques as IT environnment protects the safety and reliability of system technologies that control physical processes in a wide range of industries. Critical infrastructure like manufacturing systems, energy grids, and transportation networks etc. Are the areas where security breach could result in significant damage. It also applies in banking systems as well. It also focuses on protecting connected devices however, in a broader scale. This security measure relies on device authentication, encryption and network segmentation.

Mobile Security: Mobile devices such as tablets and smartphones have access to corporate data, exposing businesses to threats from malicious apps, zero-day, phishing and Instant Messaging (IM) attacks. This is where mobile security comes into play by providing protection to the mobile devices against these attacks and preventing unauthorised access from jailbreaking and rooting.

GenAI Security: this type of security provides protection against the use and integration of generative AI tools. The adoption of generative AI has produced many new attack vectors for cybercriminals to exploit. This security includes a list of the top 10 risk such as prompt injection, sensitive information Disclosure, Supply Chain, Data and Model Poisoning Improper Output Handling etc., and mitigations for LLMs and Gen AI Apps.

Secure Access Service Edge (SASE): It combines both networking and security into a single, unified platform based on cloud-delivered services. SASE may a combination of a Software-Defined Wide Area Network (SD-WAN) with modern security technologies such as Secure Web Gateway (SWG), Cloud

Access Security Broker (CASB), Firewall-as-a-Service (FWaaS) and Sero Trust Network Access (ZTNA).

Managed Security Services (MSS): It is a form of cybersecurity delivered and operated by a third-[arty provider. By outsourcing cybersecurity, organisations can receive dedicated services from subject matter experts who remain up-to-date on the latest trends and developments in the field. MSS security capabilities vary depending on the vendor but can include real-time monitoring for threats, vulnerability assessment and remediation processes to limit the impact of an attack.

VIII. Cyber Security: Role of AI as a Protector

Artificial Intelligence (AI) is revolutionising cybersecurity, providing tools and techniques that can detect, prevent, and respond to cyber threats with unimaginable speed and precision. The current cybersecurity systems on the market, driven by AI capability, can automatically detect anomalies, classify malicious activities, and react to threats at machine-speed. Such capacities drastically drive down detection and response time, improve scalability, and facilitate, in general, continuous surveillance of complex digital situations: cloud infrastructures, enterprise networks, and important frameworks[38].

AI empowers security professionals to defend against increasingly sophisticated attacks. In the context of cybersecurity, AI is employed to replicate or augment human decision-making processes in the detection, analysis, and response to cyber threats.[39] In practice, AI has become an essential tool in various areas of cybersecurity, notably in:

- Threat Detection and Anomaly Identification: AI continuously monitors system and network behavior. It detects deviations from established

[38] Oluwatosin Aramide, *AI-Driven Cybersecurity: The Double-Edged Sword of Automation and Adversarial,* INTERNATIONAL JOURNAL OF HUMANITIES AND INFORMATION TECHNOLOGY, Vol. 4(4), (2022) https://www.researchgate.net/publication/393600319_AI-Driven_Cybersecurity_The_Double-Edged_Sword_of_Automation_and_Adversarial_Threats

[39] C. Gilbert and M. A. Gilbert, "The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges," 2024, doi: 10.11216/gsj.2024.09.229721.

baselines, such as irregular login times or large data exfiltration, enabling early threat identification [11].

- Phishing Detection: Leveraging Natural Language Processing (NLP), AI can analyze the content and metadata of emails to identify phishing attempts by detecting patterns like spoofed senders, deceptive URLs, and manipulative language [8].
- Malware Analysis: AI examines the behavior of unknown files, including system interactions and privilege escalations, to identify malware—even those with obfuscated or zero-day characteristics [6]. • User and Entity Behavior Analytics (UEBA): By profiling normal user behavior like login frequency, time of access, command history, AI can detect suspicious deviations that may indicate compromised accounts [12].
- Automated Threat Response: Through AI-powered Security Orchestration, Automation, and Response (SOAR) platforms, organizations can automatically respond to detected threats. For example, compromised devices may be isolated from the network, or predefined scripts may be executed to contain the incident.

Nevertheless, the development of the cybersecurity field with the help of AI does not seem to be risk-free. Various evidences indicate that malicious actors are exploiting the same AI methods in defending the digital systems. Adversarial AI The newest addition to this battlefield, and one that poses potential problems in AI and ML alike, is the implementation of AI and ML by attackers to mislead or otherwise subvert defenses[40].

IX. Conclusion

The use of AI technologies by the terrorist groups to increase operational effectiveness poses a serious challenge to the government which needs to be addressed with utmost caution to curve the menace of cyber terrorism. As more

[40] Oluwatosin Aramide, AI-Driven Cybersecurity: The Double-Edged Sword of Automation and Adversarial, International Journal of Humanities and Information Technology, Vol. 4(4), (2022) available at: https://www.researchgate.net/publication/393600319_AI-Driven_Cybersecurity_The_Double-Edged_Sword_of_Automation_and_Adversarial_Threats

and more reliance is based upon the digital world in the era of digital explosion, protection of such world is the need of the hour. The ubiquitous nature of technology in all aspects of human endeavor has dramatically changed societies and economies with a consequence of increasing number of cases of cyber terrorism, one of the most alarming global threats. This alarming situation if not adequately protected in coming time, is disastrous to loss of lives and life. Each government and security agencies can employ AI-enabled advanced analytics, surveillance techniques, and predictive modelling to disrupt terrorist attacks and dismantle terrorist networks. It has become a pressing issue due to the deficiency of a consistent international treaty and the lack of international resolve. The increasing incidents of cyber-attacks against sovereign states and their critical information infrastructures necessitate a global response. Regional and bilateral agreements and local legislation are not sufficient to deter cyber-attacks. Therefore, international law is a necessary tool to enable the global community to deter cyber threats in its various jurisdictions[41].

[41] P. M Tehrani, N. A Manap & H. Taji, Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime, SciVerse Science Direct, Elsevier, Computer Law & Security Review, (June 2013), available at: https://www.researchgate.net/publication/257101606_Cyber_terrorism_challenges_The_need_for_a_global_response_to_a_multi-jurisdictional_crime