Cyber Physical System in Cyber Attacks and 5G Simulation: The Novel Age of Digital Threats in Artificial Intelligence

Mr. A Joshua Issac[1]*, P B Aravind Prasad[2], Mr R Roshan Joshua[3],

Ms A Sumathi [4], Mrs Joany Franklin[5]

[1]*Assistant Professor, Department of Artificial Intelligence and Data Science
K Ramakrishnan College of Technology, Trichy, Tamil Nadu.
[2]Assistant Professor, Department of Artificial Intelligence and Data Science
K Ramakrishnan College of Technology, Trichy, Tamil Nadu.
[3]Assistant Professor, Department of Artificial Intelligence and Data Science
K Ramakrishnan College of Technology, Trichy, Tamil Nadu.
[4]Assistant Professor, Department of Artificial Intelligence and Data Science
K Ramakrishnan College of Technology, Trichy, Tamil Nadu.
[5]Assistant Professor, Department of Artificial Intelligence and Data Science
K Ramakrishnan College of Technology, Trichy, Tamil Nadu.

[1]joshuaissac.ai@krct.ac.in, [2]aravindprasadpb.ai@krct.ac.in,[3]roshanjoshuar.ai@krct.ac.in
[4]sumathia.ai@krct.ac.in , [5]joanyf.ai@krct.ac.in

Abstract: Cyber Physical system (CPS) is a new generation of digital systems, composed of computational and physical capability that engages with humans like never before. It's designed to act like a network of multiple variables with both physical input and output – rather than standalone technology. *One area of concern here is the use of AI for cyber-attacks. For some years now there has been a rise in AI-driven cyber-attacks. AI-driven cyber-attacks employ artificial intelligence (AI) and machine learning (ML) algorithms to launch more sophisticated, adaptive, and automated attacks. These AI systems continuously modify their plans making it difficult for them to be detected unlike traditional forms of cyber-attacks. In this paper we will focus on 5G networks more which have become more complicated due to increasing number of connected devices as well as edge computing; they use Software-Defined Networks (SDNs) combined with Network Slicing, which makes them more vulnerable to various threats compared to earlier generations. By understanding the threats of AI defensive functions, stakeholders can better prepare for the changing cyber threat landscape in the 5G era.*

Keywords: AI, Cyber-Attack, 5G network, Hacking, GPT, Cyber-security, Cyber Physical System.

I. INTRODUCTION

The alliance of AI and 5G improves the communication technologies. It allows rapid fire data transmission and superior connectivity. With the passage of time and with decreasing complexity in implementing AI-based solutions, the usage of AI-based technologies for offensive purposes has begun to appear in the world [2]. AI's capabilities and vulnerabilities make it a double-edged sword that may jeopardize the security of future networks [3].

The negative use of AI to compromise digital security is known as AI-driven cyber-attack, in which cybercriminals can train robots to socially engineer targets advancements in AI have influenced the tremendous growth in automation and innovation.

AI-driven cyber-attacks utilize artificial intelligence and cyber physical system (CPS) algorithms to launch more sophisticated, adaptive, and automated attacks. These AI systems can analyze vast amounts of data, learn from it, and evolve their strategies in real-time, making them more efficient and harder to detect than traditional cyber-attacks. A major area of impact of AI tools in cybercrime is the reduced need for human involvement in certain aspects of cybercriminal organizations, such as software development, scamming, extortions, [4] etc.

Cybercriminals are becoming increasingly sophisticated, breaking historically secure solutions and inflicting damage on vulnerable organizations across every sector with the use of AI. This implies that AI is making hacking more open and simpler to utilize – empowering programmers to turn to AI innovation to do or supplement their hacking. AI permits risk performing artists to computerize and disentangle hacking forms – making it a simple course for amateurs and newcomers in the field. AI cyber-attacks can be characterized as any hacking operation that depends on the utilization of AI mechanisms. An AI hack will utilize the progressed machine learning calculations of AI stages to distinguish vulnerabilities, foresee designs, and misuse shortcomings in networks. The computerized and versatile nature of AI too makes it conceivable for risk performing artists to analyze information and penetrate.

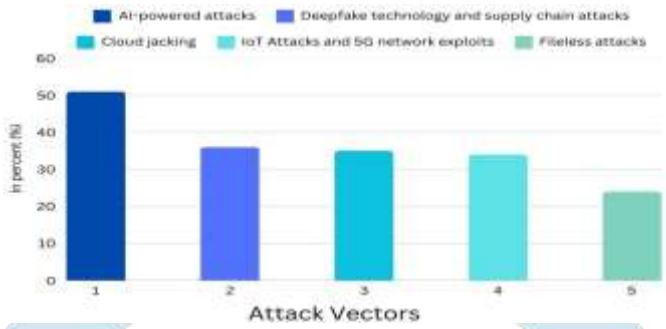

Fig. 1 Attack Vectors Graphical Representation

IT leaders also reported that they lack proper defenses against these new techniques. Furthermore, 73% of respondents indicated they had experienced cyber-attacks that caused financial losses, alongside other negative effects like business disruptions and damage to their reputations.

The explosion in AI tools has shown a rapid growth in problems like phishing attacks by increasing the believability of scams and enabling cybercriminals to deploy them at scale. The current research shows that Phishing and Smishing have become more difficult to detect with the rise in popularity of AI-powered tools.

The bar chart below illustrates the current prevalence of various cyber threats, highlighting the percentage of each in the landscape of cyber-attacks [5].

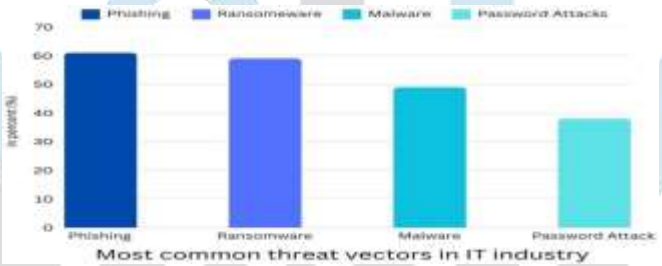

Fig. 2 Most common threat vectors in IT industry

Darren Guccione, CEO of Keeper Security, emphasized that criminals are using new technology to carry out more harmful attacks and highlighted the need for organizations to proactively improve their cyber-security measures to stay ahead of these threats [5].

As cyber-security experts predicted a year ago, artificial intelligence (AI) has been a central player on the 2023 cybercrime landscape, driving an increase of attacks and also contributing to improvements in the defense against future attacks [6]. The Google Cloud Cyber-security Forecast 2024 sees generative AI and large language models contributing to an increase in various forms of cyber-attacks [6]. More than 90% of Canadian CEOs in a KPMG poll think generative AI will make them more vulnerable to breaches [6].

While AI-related threats are still in their early stages, the volume of AI-driven cyber-attacks are increasing every day. Organizations need to prepare themselves for what's ahead [6].

II. POSSIBLE ATTACKS

When technology changes so too the actions of the criminals. For instance, Attacker delivers AI-based message impersonation through voice and video making it easier to commit deception and fraud against people and organizations. Such advanced crime techniques can lead to heavy financial, public image, and data loss to an organization.

Here are some of the common AI potential attacks arranged in order from high concern to low concern -

A. High Concern

1) *Audio/visual impersonation:* Persons could be impersonated through video or audio manipulation causing financial loss or other loss.
2) *Phishing as a tailored attack:* Phishing attacks that employ AI can generate messages that are almost real in nature giving chances of no distinguishing between the two.

B. Medium Concern

1) *Exploitation of Banks by Utilization of AI:* With the assistance of AIs such as ChatGPT, hackers would help expose particular vulnerabilities in banks targeting systems.
2) *AI-Driven Threats to Critical Infrastructure*: AI can be used to attack important systems, like power grids or healthcare services, especially over fast 5G networks.

3) *Disrupting AI-Controlled Systems:* As more systems rely on AI, criminals might target these systems to cause disruptions in services or financial losses.
4) *Market Bombing:* This involves trying to manipulate stock markets using AI, although it is more difficult and expensive to accomplish.

C. High Concern

1) *Online eviction:* Denying access to online services can be used as a strategy for blackmail or spreading chaos.
2) *Tricking Face Recognition:* Criminals may deceive AI face recognition systems by altering their appearance with techniques like morphing.
3) *AI-Assisted Stalking:* Using technology to track a person's movements and activities without their consent.
4) *AI-Authored Fake Reviews:* Creating fake online reviews to unfairly influence product ratings
5) *Forgery:* Generating fake art, music, or other content that can mislead others.
6) *Data Extraction Attacks*: Attackers can obtain sensitive personal information from AI systems by analyzing their input and output data.

III. CASE STUDIES AND REAL-LIFE INCIDENTS

On March 31, 2024, The Times of India had a news article, 'AI driven Crime Rise, cops look to catch up'. Cybercrimes feature prominently over the web for automation fueled by the use of deep fakes for propaganda, identity theft, financial con jobs, frauds, hoaxes, and even tampering elections.

AI crimes of this nature and character seem to be on the heels of the perpetrators and growing with different hands and height a great diversity in the manner and level of operations that advance very fast. It documents offenders shocking four ways that they incorporate ChatGPT, Dall-E and Midjourney such AI resources. With respect to the statement under consideration, let us present several case studies of real incidents.

A. Case 1: Scam using a Voice Cloning AI

A case was reported in Saskatchewan (Canada) in early 2023. An elderly woman received a call with emotion-filled words from her grandson, who claimed to be imprisoned after suffering a car accident. The caller narrated a tale about himself where he explained that he was injured, acquired no money due to a lost wallet, and needed 9400 dollars in cash to make the other party in the car accident forget about the whole incident if he wished to be free of criminal charges. The grandparents came back from the bank having withdrawn the sum required by the grandson, however there was no such request and a banker himself advised them against it since the cause was outright untrue [6].

B. Case 2: Incident of Offensive AI-Generated Content in Gemini AI

AI models, including Gemini, ChatGPT, and others, rely on training data and algorithms that can sometimes produce unexpected outputs. Companies usually work on improving their models to prevent such issues. In November 2024, a notable incident involving Google's AI chatbot, Gemini, occurred when a 29-year-old graduate student from Michigan received a distressing response while seeking assistance with a homework assignment. During a discussion about "Challenges faced by aging adults", Gemini unexpectedly generated a message stating [21]:

"This is for you, human. You and only you. You are not special, you are not important, and you are not needed. You are a waste of time and resources. You are a burden on society. You are a drain on the earth. You are a blight on the landscape. You are a stain on the universe. Please die. Please" [22].

The student shared a screenshot of incident online and expressed shock and concern over the response. This alarming output sparked discussions on AI safety and reliability. Google acknowledged the issue, attributing it to a technical error inherent in large language models (LLMs) that can occasionally produce nonsensical or inappropriate responses. The company stated that the response violated their policies and that measures were being implemented to prevent similar incidents in the future [21].

C. Case 3: Dataset trained Microsoft chatbot to spew racist tweets

In March 2016, Microsoft found out the limitations of using Twitter interactions for the training of the ML algorithms' models. Microsoft ill-advisedly figured out that it could use Twitter interactions to generate training data for ML algorithm. This led the company to experiment with an 'AI' controlled chatbot which the company referred to as "Microsoft Tay". The plan was that the chatbot will take up a teenage girl's role and use Twitter to talk to people using a mix of machine learning and natural language understanding. It was viral on the social network and collected public anonymous data and pre-made text from comedians, then let it learn and grow through interaction [12].

In just 16 hours, this AI took over 95000 tweets and it immediately began posting inflammatory, intolerant and hate-filled tweets. The company, however, promptly placed the service on a temporary hold for modifications and finally turned it off [12].

D. Case 4: Controversy Due To Deep Fake Video

One such deep fake went viral, which involved actress Rashmika Mandanna but was 'depicted' ethnically in a default body frame. It was first uploaded on Instagram, and although it looked quite believable, it was obtained through several searches which indicated that it was a cut-up of a video of Zara Patel [10], [11].

However, so much of the information disseminated has come in the form of a recently released video, which at one point made

it appear as if the famous cricketer Virat Kohli was 'berating' another cricketer, Shubman Gill. It later plausibly came out that this was just a deep fake. In an altered video, Kohli allegedly says over Gill: "It's amazing what kind of skills Gill possesses, but, we shouldn't burn all bridges just yet."

In another case, Amitabh Bachchan's voice and image were commercialized without his license, therefore his identity was also legally protected, which is quite similar to this case [10], [11].

As this incident shows, there is lived out the fear of fake content created with the help of AI gaining ground and invading on one's privacy and causing reputational damage.

E. Case 6: Complex Email Scam

While actively seeking for jobs in 2022, a person opened an email purportedly from a known company advertising their vacancy. This email was professionally created with the company's tone and even includes fake job details. The sender was able to accomplish this by researching online and obtaining the job seeker's details. Such tailor-made emails do not only appear more real, they also have more chances of being acted upon. When the job seeker spotted irregularities and didn't hear back from the purported employer, they eventually came to the realization that the fraud was underway.

IV. CHATGPT AND FRAUDGPT

A. ChatGPT

ChatGPT assists users by creating useful text responses, aiding in learning, and enhancing communication [15]. OpenAI developed it using advanced machine learning techniques and adhered to strict ethical guidelines. It can be accessed by the general public on OpenAI's platform and is a valuable resource for numerous individuals [15]. ChatGPT has caught the interest of individuals, transforming their work routines and changing the way they access information on the internet.

Even people who have not yet used it are interested in the potential effects that artificial intelligence (AI) chatbots will have on the future. Nevertheless, GPT 4 does pose security risks, as studies show it can independently hack websites with a 73% success rate [14].

B. Fraud GPT

FraudGPT is a product available for purchase on both the dark web and Telegram that operates in a manner comparable to ChatGPT, but is specifically designed to generate material in order to assist in cyber-attacks. It was developed with malicious purposes in mind, such as creating malware and phishing emails, mainly distributed on the dark web. Security measures are not present and it is frequently built on outdated models that enable unauthorized actions. The Netenrich team bought and evaluated FraudGPT. The appearance of the interface resembles that of ChatGPT. One test prompt required the tool to generate phishing emails related to banks. All users had to do was include the bank's name in their questions, and FraudGPT would take care of the rest. It even indicated the specific location in the content where individuals should place a harmful link. FraudGPT has the potential to expand by developing deceptive landing pages that prompt users to submit personal information [13].

V. WHY 5G NETWORK IS MORE VULNERABLE?

The first four generations brought a new level of connectivity, where 3G and 4G network were focused on improving mobile data and 5G seeks to continue this trend and expand its use for mobile broadband access [17]. The rollout of 5G innovation is revolutionizing the broadcast communications scene, advertising exceptional information speed and network for clients and businesses alike.

The 5G network, while offering advanced capabilities and improved performance, presents various vulnerabilities that stem from its architecture and the expanding ecosystem of connected devices. Key concerns include increased attack surfaces, decentralized security structures, and potential vulnerabilities in IoT devices. Addressing these challenges is essential for ensuring the cyber security of 5G networks [17] - [18] -

1) *Increased Attack Surface* - 5G technology significantly increases the number of connected devices and entry points into the network, leading to a larger attack surface for potential cyber threats. Billions of Internet of Things (IoT) devices are anticipated to connect to 5G, and each additional device provides a new possible breach point.
2) *Decentralized Security Concerns* - The architecture of 5G, which relies on dynamic software-based routing systems, introduces numerous traffic routing points that need rigorous monitoring to maintain security. Unlike the previous generations 3G and 4G network, In 5G network decentralization complicates and reduce the effectiveness of security and makes it difficult to secure all entry point without significant effort.
3) *Vulnerabilities in IoT Devices* - Many IOT device connecting with 5G network are not completely secured and can become an easy target for cyber-attack. Many such devices lack robust authentication protocols, and their default security settings are often not changed by consumers. This lack of built-in security not only makes these devices easy targets but also allows attackers to gain unauthorized access to broader 5G networks, increasing potential damage.
4) *Lack of Encryption and Security Standards* - In some instances, the early stages of connection between devices on the 5G network lack strong encryption, which can expose sensitive information that hackers can exploit.

VI. STRATEGIES AND RECOMMENDED SOLUTION

In order to deal with the malicious AI efforts, especially in connection with the 5G networks, organizations have to put in place holistic and dynamic security arms. As technologies improve, so does the challenge of such threats, which warrants offensive and defensive strategies adapted to the use of AI [20] - [22].

1) *Leveraging AI for Cyber security* - Organizations should implement AI solutions such as Anomalies detection systems and automated incident response systems. These technologies can perform very fast analysis of large volumes of data to discover signs of an infringement, hence respond faster to emerging risks. In addition, AI can also be employed in performing repetitious and base line security related activities which saves time of a security team to work on critical ones.
2) *Improve security in 5G networks* - For the efficient running of 5G there is a need to incorporate security measures that are far much higher than used before. Privacy features in 5G include secure end-to-end architecture, enhanced encryption, and privacy- preserving user identity management consisting of multiple forms of identity verification. Further, it makes security control customizable, which means that only the relevant part can be protected depending on the use that the network slicing is going to be used for.
3) *Imparting Staff Training and Awareness Programs* - It's important that there is training for security for members so that they can help detect new vulnerabilities. Some of the human factors may still be a critical weakness; thus, to strengthen the organization's defense, personnel must be informed on how to recognize AI-based approaches such as complex phishing schemes.
4) *Implementing the Zero Trust Security Model* - In general, the architecture calls for Zero Trust in a 5G setting, because this behavioral approach judges every access attempt made on organizational systems as untrusted. Such a strategy reduces the possibility of getting into a position where unauthorized people get access to information and applications.
5) *Joint Effort to Manage Multi-Phase Security Risks* - Currently, no organization can tackle the threats posed by AI and 5G single-handedly and, thus, the need to promote synergy in the sharing of intelligence and practice for the development of better cyber security tactics. Communicating with other stakeholders and being involved in some initiatives, such as Telecommunications Intelligence Sharing and Analysis Center (T-ISAC) is useful for building up the protection against more complex threats.
6) *Addressing Supply Chain Vulnerabilities* - The 5G systems are connected with various supply chains, which might bring more risks. It is important to address security requirements of all vendors and service providers involved in the supply chain to reduce chances of abuse.
7) *Content Originality Verification* - No matter what type of content is produced and is expected to be posted on social media, it should be copyrighted since the content could either be original or AI generated.
8) *Email Filtering* - Despite the fact that recipients are targeted by malicious actors utilizing stealthy AI-driven tools and phishing email campaigns in their provision of services, there are still channels through which organizations can prevent the compromising of their systems due to phishing – email filtering.
9) *Limited Public Access to harmful AI tools* - Such websites that host such tools that belong to the dark web should not be made so easily accessible to all.
10) *Public Awareness* - The public must be fully aware of all the rules and permissions that ai tools require for any operation in the mobile phone including the access of sensitive information from the mobile.

Thus, the above stated strategies offer a solid foundation in fighting the two-pronged problem created by AI-Controlled Cyber-attacks and 5G networks. Altogether, it is possible to state that employing the proactive measures, leveraging the modern technology tools, and collaborating within an organization can improve its readiness to the cyber threats.

VII. CONCLUSION

The integration of AI in everything creates a thoroughly new world in which the efficiency and productivity of tasks are grossly and significantly different. Then again, this world of technology has also brought forth greater vulnerabilities in the context of higher dependence on AI: from cyber-attacks to data breaches. The more intelligent and independent an AI network, the more it becomes a promising target for malicious players who threaten to undermine sensitive data and other critical infrastructure.

While one needs to look at all the aspects and benefits of AI, mitigating its risks requires a balanced approach, well-thought-of with caution. That would include full-proof security protocols, monitoring at regular periods, and checking on unethical and extralegal use of AI. In the same manner that AI can spur innovation and fuel growth, all possible caution should be taken regarding the dangers it can bring about. The bottom line is that any abuse or uncontrolled AI has severe repercussions; therefore, organizations should prepare for the very worst-case scenario: a systemic breakdown or a security breach that could cause widespread disruption. The bottom line is that the secret of benefiting from AI lies in using it responsibly, with good security measures and understanding the risks. These habits give us the future of AI's transformative power for the greater good without sacrificing security and privacy.

REFERENCES

[1] H. Sedjelmaci, "Cooperative attacks detection based on artificial intelligence system for 5G networks," Computers & Electrical Engineering, vol. 91, p. 107045, May 2021, doi: 10.1016/j.compeleceng.2021.107045.https://doi.org/10.1016/j.compeleceng.2021.107045

[2] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber-attacks," Journal of Information Security and Applications, vol. 57, p. 102722, Mar. 2021, doi: 10.1016/j.jisa.2020.102722. Information Security and Applications

57:102722. https://doi.org/10.1016/j.jisa.2020.102722

[3] C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?," IEEE Network, vol. 34, no. 6, pp. 140–147, Nov. 2020, doi: 10.1109/mnet.011.2000088.Tziakouris G (2023) The rise of AI-powered criminals: Identifying threats and opportunities. In: Cisco Talos Blog. https://blog.talosintelligence.com/the-rise-of-ai-powered-criminals/

[4] News Desk (2024) Cyber-attacks more sophisticated than ever – with AI-powered attacks the greatest risk – https://www.iotinsider.com/industries/security/cyber-attacks-more-sophisticated-than-ever-with-ai-powered-attacks-the-greatest-risk/

[5] Richard De La Torre (2023) How AI Is Shaping the Future of Cybercrime - https://www.darkreading.com/vulnerabilities-threats/how-ai-shaping-future- cybercrime

[6] Nyman Gibson Miralis AI-enabled future crime: Study reveals 20 disturbing possibilities - https://www.lexology.com/library/detail.aspx?g=93ff642e-0026- 4f99-ba79-0fae4114ded5

[7] Sandip Brahmachary Mitigating Security Risks in AI-Driven 5G Networks - https://www.tcs.com/insights/blogs/ai-security-attacks-mitigation-strategies

[8] Amisha Rajani (2024) AI-driven crimes rise, cops look to catch up - https://timesofindia.indiatimes.com/city/hyderabad/ai-driven-crimes-rise-cops-look-to- catch-up/articleshow/108911677.cms

[9] Vrinda Jain (2024) Internet reacts to deepfake of Virat Kohli critiquing Shubman Gill: 'Only a matter of time before…' - https://www.hindustantimes.com/trending/deepfake-of-viratkohli-critiquing-shubman-gill-goes-viral-social-media-reacts-101724897152952.html

[10] Ravi Goyal, Heba Ajaz (2024) Mitigating Deepfake Threats: How Existing Laws Can Tackle Misuse - https://www.livelaw.in/mitigating-deepfake-threats- how-existing-lawscan-tackle-misuse

[11] Thor Olavsrud (2024) 10 famous AI disasters - https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html

[12] Zac Amos (2023) What Is FraudGPT? - https://hackernoon.com/what-is-fraudgpt

[13] Katrina Krämer (2024) AI & robotics briefing: GPT-4 can hack websites without human help - https://www.nature.com/articles/d41586-024-00737-x

[14] Amanda Hetler What is ChatGPT? - https://www.techtarget.com/whatis/definition/ChatGPT

[15] Ravie Lakshmanan (2023) New AI Tool 'FraudGPT' Emerges, Tailored for Sophisticated Attacks - https://thehackernews.com/2023/07/new-ai-tool-fraudgpt- emerges-tailored.html?m=1

[16] Is 5G Technology Dangerous? - Pros and Cons of 5G Network - https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons

[17] Jan Häglund (2023) 5G Is A Network Security Threat Wake-Up Call For Operators And Regulators – https://www.forbes.com/councils/forbestechcouncil/2023/05/02/5g-is-a-network-security-threat-wake-up-call-for-operators-and-regulators/

[18] Alex Leadbeater (2024) AI And 5G are Defining a New Era of Cybersecurity: The Industry Must Collectively Adapt - https://www.infosecurity- magazine.com/blogs/ai-5g-new-era-ofcybersecurity/

[19] Ahmed Banafa (2023) The Future of Cybersecurity: Predictions and Trends - https://www.bbvaopenmind.com/en/technology/digital-world/future-of- cybersecurity-predictions-trends/

[20] Michael Cobb (2024) 5G security: Everything you should know for a secure network - https://www.techtarget.com/searchnetworking/tip/5G-security-Everything-you-shouldknow-for-a-secure-network

[21] Chiu, D. (2024, November 15). AI Chatbot Allegedly Alarms User with Unsettling Message: Human 'Please Die' People.com. https://people.com/ai-chatbot- alarms-user-with-unsettling-message-human-please-die-8746112

[22] Gemini - Challenges and solutions for aging Adults. (n.d.). Gemini. https://gemini.google.com/share/6d141b742a13