Risk of Dual Use Artificial Intelligence in Genetic Engineering

Rosa Syafitri and Teddy Mantoro

June 27, 2025

Risk of Dual Use Artificial Intelligence in Genetic Engineering

Rosa Syafitri[1], Teddy Mantoro[1,2]
[1]*Post Graduate School of Medical Intelligence, State Intelligence College,* Bogor, Indonesia
[2]*School of Computer Science, Nusa Piutra University, Sukabumi,* Indonesia

***Abstract*— The integration of Artificial Intelligence (AI) and genetic engineering is transforming modern biotechnology, with significant impacts on medicine, agriculture, and manufacturing. However, this integration also raises serious biosecurity risks, especially due to the potential for dual-use applications of AI in genetic engineering. This study offers a thorough assessment of these biosecurity risks, examining how AI could be misused to create biological threats, such as engineered pathogens or bioweapons, that might endanger national security. It evaluates vulnerabilities in AI-driven genetic technologies and the potential misuse by both state and non-state actors. Through this risk assessment, the study suggests strategies for mitigating these risks, including the development of AI-specific biosecurity guidelines, increased international collaboration, and the implementation of advanced monitoring systems. The findings underscore the urgent need for proactive measures to protect against the misuse of AI in genetic engineering, ensuring that the benefits of these technologies do not come at the expense of security.**

Keywords*— *Genetic Engineering, Artificial Intelligence, Biosecurity, Dual-Use, Risk assessment.

I. INTRODUCTION

The discovery of CRISPRs (Clustered short palindromic repeats) has led to a revolution in biotechnology. The CRISPR-Cas9 system can be programmed to edit parts of the genetic code in specific part, and replace them in the genome in a matter of hours. This gene editing technology expand the possibilities of genetic engineering such as inserting new DNA sequences, either natural or completely new, into specific genome of an organism. If the changes are made in the germ line, this can become hereditary. CRISPRs-Cas9 has enable the design and automation of genetic engineering, making it cheap, fast and accurate. Do-it-yourself bacterial genome CRISPRS kits are available online, scientist often custom DNA sequence from commercial labs (mail-order DNA and DNA printer) [1].

The integration of Artificial Intelligence (AI) with genetic engineering has caused significant advances in modern biotechnology [2]. However, there is an increase in biosecurity risk, particularly due to the dual use potential of AI in genetic engineering. Dual-use technology refers to innovations that, while intended for beneficial purposes, can also be repurposed for malicious applications. As AI aids in the rapid identification, modification, and synthesis of genetic material, there is a growing concern over the possible misuse of these capabilities, particularly by state and non-state actors with malicious intent. This dual-use potential raises concerns about the creation of engineered pathogens, the enhancement of biological weapons, and the deliberate or accidental release of harmful organisms [3]. This article aims to provide a comprehensive risk of biosecurity threats posed by the integration of AI in genetic engineering, along with strategies to mitigate these risks.

II. RELATED WORK

Genetic engineering in the era of synthetic biology expands the range of potential safety concerns. The Risk Assessment framework used by National Academies of Science, Engineering, and Medicine (NASEM) in assessing synthetic biology level of concern about their capabilities and implications consists of four factors: 1) Usability of the Technology, 2) Usability a Weapon, 3) Requirements of Actors, and 4) Potential for Mitigation. Limitation in using this approach to combine AI and biotechnology risks is that its scope is limited and restricted to risks from synthetic biology and technologies [4].

Hybrid Risk Assessment framework used by O'Brien uses several critical parameter such as: democratization, vulnerability, needed skill and expertise, governability, magnitude of potential consequence, and existing countermeasure. In order to enhance specificity the framework use various specific scenarios [5].

Risk assessment paper by Sandbrik specifically analyze risk involving specific AI model: Large Language Model (LLM) dan Biological Design Tool (BDT) and the convergence of the two model that increase the risk level [6].

Recent Biosecurity risk assessment procedure used by De Haro assess vulnerabilities and threats, evaluate AI system level of maturity and automatization, determine consequence and risk level based on probability and severity [7]. This study used Hank Prunckun Method of intelligence analysis, which is adapted in this paper to allows measurable quantitative risk analysis from the aspects of threat, vulnerability, and risk level. Risk can be placed in risk assessment matrix to be compared with each other to prioritize treatment options.

III. METHOD

Literature review, was carried out to gather information, as the application of AI in the field of genetic is a new development. A literature review using the search terms "generative AI", "synthetic biology", "genetic engineering", "genome editing" and "AI" in Google Scholar, SCOPUS, PubMed, and Science Direct. No human data was collected for this study.

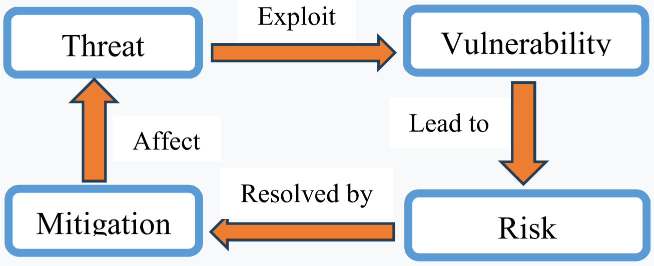


Figure 1. Conceptual Framework

The risk analysis method used in this paper is Hank Prunckun's method as outlined in his book Methods of Inquiry for Intelligence analysis [8]. As presented in Figure 1, the method used by Hank Prunckun consists of:

A) Threat Assessment

A threat is the desire of one person to harm another. Threat can be made against individual, group, and countries by a threat agent. A threat actor with *Intent* and *Capability* must have the ability to do harm. *Intent* can be defined as the threat actor's optimism that an attack against the target will be successful, and *Capability* as the extent of the threat actor's ability to exert on the target. Threats are expressed as an equation [8]:

$$\textbf{\textit{(Desire + Expectation) + (Knowledge + Resources) = Threat}} \quad (1)$$

Desire can be defined as the eagerness of a threat actor in pursuing his or her goal. *Expectation* is the threat actor confidence in its ability to achieve its objective if its plans are occurred. *Knowledge* is the possession of information that will enable the threat actor to use or to build the tool or to perform the necessary steps to achieve his or her objectives. *Resource* includes the skill (or experience) resources required to act according to a person's plan. Threat coefficient is calculated by adding *Desire* and *Expectation*, this sum is added to the sum of *Knowledge* and *Resources.* Each of *Desire, Expectation, Knowledge, and Resources* was scale from 1-5 (1: negligible, 2: minimum, 3: medium, 4: high, 5: acute). The coefficient obtained from this analysis is compared to a reference chart to determine where it fits into attack risk spectrum. (1-3: negligible, 4-6: minimum, 7-9: medium, 10-12: acute, 13-15: high, 15-20: extreme) [8].

B) Vulnerability Assessment

Vulnerability could be defined as a weakness in an asset that threat actor can exploit. In this context, asset means a resource that needs protection. A resource can be a person, a group of people or a physical object. Vulnerability is the ability of assets to withstand damage caused by threats. The damage can be of any kind, from a minor problem to a catastrophic situation.

Vulnerability is a function of several factors: a) attractiveness of the target, b) ease of attack (possibility of a successful attack), and c) potential impact (possibility of damage and loss). Hank Prunckun's way of calculating vulnerability is like [8]:

$$\textbf{\textit{Attractiveness + Ease of attack + Impact = Vulnerability}} \quad (2)$$

Each point of Attractiveness, ease of attack and impact was scale form 1-5 (1: negligible, 2: minimum, 3: medium, 4: high, 5: acute). All of the point was summed to calculate vulnerability coefficient with scale 1-15 (1-3: negligible, 4-6: minimum, 7-9: medium, 10-12: high, 13-15: acute) [8].

C) Risk Assessment

Risk is the effect of uncertainty in something. Risk assessment consist of risk analysis and risk evaluation. Risk management (Risk Mitigation) refers to coordinated activities to guide and control the organization in terms of risk. Risk is a function of *Likelihood* and *Consequence*. This article analyze the risk with equation [8]:

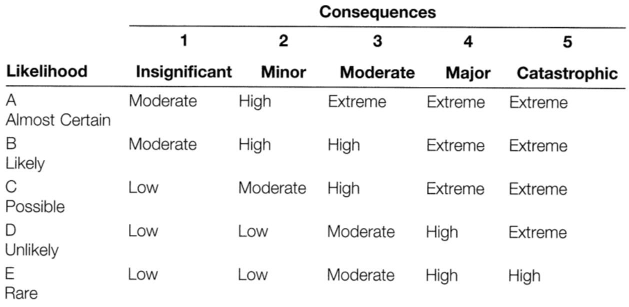
$$\textbf{\textit{Risk = likelihood + consequence}} \quad \textit{(3)}$$

Likelihood refers to probability of a particular event or outcome, measured by the number of events or outcomes relative to the total number of possible events or outcomes. *Likelihood* was rank from A-E range from Almost certain (A) where the condition is expected to occur, to Rare (E) where the condition only occur in exceptional circumstances. *Consequences* are defined as the result of activities that affect things. *Consequence*s were rank from 1-5, from insignificant (1) when they have a low impact to catastrophic (5) when they cause system or operation to fail with high impact [8].

D) Treating Risk (Risk Mitigation)

Risk analysis allows the researcher to recommend action to accept or deal with the risk (including decision to avoid the risk, reduce the risk, or transfer it to another person or organization). Once the risk has been assessed, the measures can be entered into risk score matrix so that they can be compared with each other to prioritize treatment options. The number provided in the risk rating is useful in deciding whether to accept the risk or deal with it [8] as shown in Table 1.

TABLE 1 Risk Rating Matrix (adapted from Hank Prunckun (2019)



	Consequences				
	1	2	3	4	5
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
A Almost Certain	Moderate	High	Extreme	Extreme	Extreme
B Likely	Moderate	High	High	Extreme	Extreme
C Possible	Low	Moderate	High	Extreme	Extreme
D Unlikely	Low	Low	Moderate	High	Extreme
E Rare	Low	Low	Moderate	High	High

IV. RESULT AND FINDING

There are 2 threat agent (AI Tool) included in analysis in this paper [1]:

1) *Large Language Model (LLMs)*, like GPT-based systems, can process vast amounts of information and generate human-like text. In genetic engineering context, they could be used to gather, synthesize, or interpret biological research. *LLM* have the potential for dual-use such as generating harmful biological instructions or aiding in dangerous bioengineering processes. LLM can improve access to biological knowledge, reducing barier to its misuse.
2) *Biological Design Tool.* Biological design tools use AI to assist in the creation of synthetic organisms, proteins, or DNA sequences. Biological design tools allow users to design and synthesize biological organisms. These tools hold immense power and are vulnerable to being used to create dangerous or harmful genetic constructs.

A. Threat Analysis of AI in Genetic Engineering

Table 2 showed that LLM in genetic engineering is a **high (15)** threat due to its ability to generate sensitive information with relative ease, which could be leveraged for malicious purposes like bioengineering harmful agents. While AI-driven BDT present an **acute (17)** threat, particularly in the hands of bioterrorists or irresponsible users. Their potential to design harmful biological agents makes them especially dangerous (See Figure 2).

TABLE 2 Threat Analysis Result

	Large Language Model (LLM)	Biological Design Tool (BDT)
	Intention Analysis	
Desire	**Score: 4 (High)** **Malicious Actors**: Cybercriminals/ bad actors may seek to use LLMs to generate harmful content, such as methods for bioengineering pathogens / designing toxins. **Non-Malicious Misuse**: Misguided individuals could use these models without fully understanding the potential consequences, inadvertently causing harm.	**Score: 5 (Acute)** **Malicious Actors**: Terrorist groups or criminal organizations may seek to use AI-driven biological design tools to engineer bioweapons or harmful organisms. **Researcher Misuse**: Incompetent or careless use by undertrained researchers could result in unintended consequences (e.g., accidental release of modified organisms).
Expectation	**Score: 4 (High)** LLMs are increasingly accurate in generating text, and malicious actors may have a high expectation of success in using these tools to generate biological data, such as DNA sequences or synthesis methods.	**Score: 4 (High)** There is a high expectation that AI-driven tools can accurately design biological sequences, whether for positive or malicious applications. These tools are advancing rapidly and are increasingly reliable.
Intent Calculation	Desire (4) + Expectation (4) = **8 (Medium-High)**	Desire (5) + Expectation (4) = **9 (Acute)**
	Capability Analysis	
Knowledge	**Score: 4 (High)** LLMs provide access to high-level knowledge, including sensitive biotechnology data from scientific paper and research method. However, the complexity of biotech tasks (e.g., gene editing) requires domain-specific expertise.	**Score: 4 (High)** Biological design tools typically require in-depth biological and chemical knowledge. AI can compensate by providing access and reducing barier, enabling malicious actors without deep expertise to design organisms.
Resource	**Score: 3 (Medium)** LLMs typically requires computational power but not specialized equipment. However, scaling up to misuse in biological contexts (e.g., synthesizing viruses) would require access to labs, tools, and funding.	**Score: 4 (High)** AI can facilitate design, but designing harmful biological agents requires lab access, equipment for DNA synthesis, and sometimes funding from malicious actors or states.
Capability Calculation	Knowledge (4) + Resources (3) = **7 (Medium)**	Knowledge (4) + Resources (4) = **8 (High)**
Threat Coefficient	Intent (8) + Capability (7) = **15 (High)**	Intent (9) + Capability (8) = **17 (Acute)**

TABLE 3 Vulnerability Analysis Result

	Large Language Model (LLM)	Biological Design Tool (BDT)
Attractiveness	**Score : 4 (High)** LLMs are highly recognizable, especially in general public & scientific communities, making them an attractive target for both legitimate use and misuse by cybercriminal.	**Score : 3 (Medium)** These tools are recognized within biotech and synthetic biology sectors but are less known outside the field.
Ease of Attack	**Score : 3 (Medium)** Public availability of LLMs via open-source models makes it easier to access. Some model have some level of security and monitoring, open-source and unauthorized use are more vulnerable to manipulation or misuse.	**Score : 2 (Minimum)** The tools require more expertise, making it harder for threat agents to exploit them. The tools are often housed within secure environments (e.g., academic labs, biotech companies). But unauthorized or rogue labs may lack sufficient controls.
Impact	**Score : 3 (medium)** Misuse of LLMs in genetic engineering could lead to dangerous mis-information or generating harmful biological process, but less immediate physical impact. Financial damage could be significant and variable resulting from data leaks, sabotage of biotech result or unethical application.	**Score : 5 (acute)** The potential to create harmful organisms or pathogens using these tools could lead to catastrophic outcomes. The financial damage could be immense, both in terms of healthcare costs and damage to the biotech industry. ▪
Vulnerability Coefficient	Attractiveness (4) + Ease of Attack (3) + Impact (3) = **10 (High)**	Attractiveness (3) + Ease of Attack (2) + Impact (5) = **10 (High)**

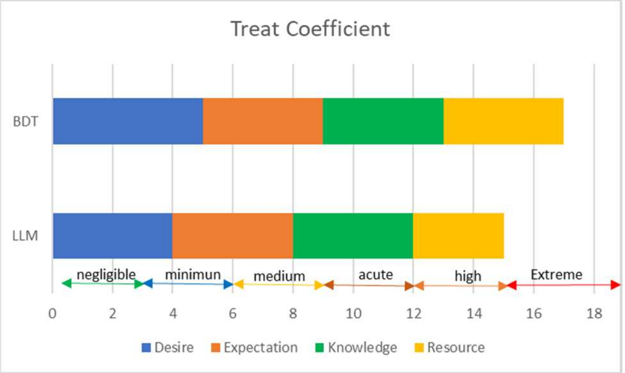


Figure 2. Treat Coefficient Result

B. *Vulnerability Analysis of AI in Genetic Engineering*

Table 3 showed that LLM pose **high (10)** vulnerability coefficient with major concern in moderate impact and wide public availability make LLM an attractive and accessible target. While BDT also pose **high (10)** vulnerability coefficient with harder to exploit tool but with potential for catastrophic human and financial impact as shown in Figure 3.

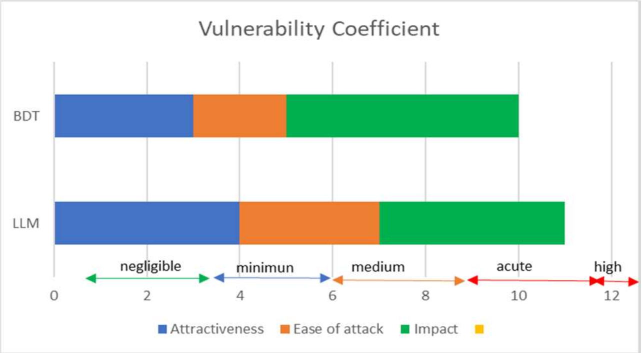


Figure 3. Vulnerability Coefficient Result

C. *Risk Analysis of AI in Genetic Engineering*

Risk of **LLM** misuse in genetic engineering is **extreme**, given the likely potential for misuse and the major consequences if harmful outcomes occur. LLMs present a significant risk due to their accessibility and ability to generate detailed biological information that could be misused. While risk of misuse of BDT is also **extreme** due to the catastrophic consequences associated with the potential creation of harmful biological agents, even though the likelihood of such misuse is lower than LLMs as presented in Table 4.

TABLE 4 Risk Analysis Result

Large Language Model (LLM)	LLMs are increasingly accessible and can be misused in certain situation by malicious actors to generate information about biological hazards (e.g., genetic sequences / instructions for creating harmful biological agents). **Likelihood Ranking**: **B (Likely)** LLMs are used to generate harmful biological instructions. It could lead to the creation or dissemination of dangerous biological agents. The outcome could range from the release of harmful misinformation to direct involvement in the development of harmful pathogens. **Consequence Ranking**: **4 (Major)** **Risk = Likelihood (B) + Consequence (4) = B4 (Extreme Risk)**
Biological Design Tool (BDT)	Biological design tools are specialized and require substantial expertise to operate. Given the complexity of these tools and the oversight they generally require, misuse is possible. **Likelihood Ranking**: **C (Possible)** Misuse of BDT can lead to catastrophic consequences, including loss of life, societal disruption, creation of pandemic level pathogen, and long-term environmental and economic impacts. **Consequence Ranking**: **5 (Catastrophic)** **Risk = Likelihood (C) + Consequence (5) = C5 (Extreme Risk)**

D. *Risk Mitigation*

Addressing the biosecurity risks of AI-driven genetic engineering requires a multi-faceted approach. Key strategies for mitigating these risks include:

1. Development of AI-Specific Biosecurity Guidelines. Guidelines must explicitly address the dual-use nature of AI-integrated biotechnology, including the potential for misuse. Guidelines should include ethical standards and inform consent for the development or use, as well as mandatory risk assessment protocols for new AI systems and requirements for comprehensive documentation and review processes.
2. Increased International Collaboration. Biosecurity is a global issue. To mitigate cross border risk, international collaboration between governments, private firm, research institution, and international security organization is essential. This includes a structured information sharing network that provide real time updates on emerging threat, coordinating biosecurity efforts, and developing joint simulation exercise and crisis responses to potential biological attacks.
3. Strengthening International Regulation. The establishment of a global oversight body is crucial to set universal standard across nations, provide licensing for AI tools used in sensitive research, and implement penalties for breaches.
4. Implementation of Advanced Monitoring Systems. Beside global surveillance, AI-driven monitoring systems could be integrated with existing biosecurity infrastructure to track unusual activity across multiple genetic databases, surveillance networks, and laboratory records. Researcher should consider developing AI tool/algorithms to detect harmful biotechnological developments with a focus in early warning system. This would provide authorities with critical time to intervene, investigate, and potentially prevent harmful applications before they are released.

V. Discussion

Revolution in genetic engineering with AI promise a dramatic increase in democratization of gene editing capabilities by enabling bioengineers to process large amounts of data, understand complex system, and conduct efficient large scale automated testing. AI help to identify virulence and in silico production new pathogen. Biotech start-up develop ESM3, generative AI for Biology that can explain structure, organization, and function of new protein in response to chatbot prompt [9]. This study also reported OpenCRISPR-1, the first human genome editing with AI programmed gene editor [10]. However, alongside the benefit there is an increase in biosecurity risk due to the dual use potential of AI in genetic engineering, particularly by state and non-state actors with malicious intent.

Canada Biosecurity scandal happened in July 2019, where a group of Chinese Virologist were forcibly expelled from Canada's National Microbiology Laboratory (NML). They were part of Canada Public Health Special Pathogen Program. One of the procedures involved infecting monkeys with Ebola, the world deadliest virus. Few months before the team was expelled, a ship carrying two infectious disease (Ebola and Nipah) was shifted from NML to China. The shipment is considered inappropriate and potentially illegal [11].

A. Potential Dual-Use of AI in Genetic Engineering

- *Engineered Pathogens and Bioweapons*

  AI-enables pathogen design can rapidly analyze genetic sequences to identify mutations that increase pathogen virulence or drug resistance, potentially creating more deadly and harder-to-detect viruses (gain of function research). This capability could be exploited to enhance pathogen lethality if accessed by malicious actors. Recent cases, such as synthetic recreations of the horsepox virus (family of small-pox) and the 1918 pandemic influenza virus, highlight the feasibility of AI-enabled pathogen synthesis [12].

- *Targeted Bioweapons*

  AI can analyze genetic data from specific population, enabling the design of pathogen tailored to certain genetic profile, raising the risk of targeted bioweapon. AI allow creation of precision bioweapons aimed at particular demographic group, facilitating the conduct of genocide at a potentially global scale. Through computational and molecular simulations, AI designs genetically specific nanobots to attack specific organ system in human body. AI could also be applied to disease-carrying vectors (e.g., genetically engineered mosquitoes) to introduce harmful genes into targeted populations [1].

- *Toxin Engineering and Chemical Weapon*

  AI enhanced capacity to engineer deadly toxin. An International security conference investigate how AI software (MegaSyn AI) involved in drug discovery could produce thousands of new chemical weapon, including VX (one of the most powerful poisons) in less than 6 hours by using open source internet data. Many of these substance are novel and not on the government watch list [13].

- *LLM Increase access to dangerous information*

  An experiment showed that student without technical training could in 60 minutes identify 4 possible pandemic pathogen. LLM can explain how they are produced from synthetic DNA, named the DNA synthesis company that might bypass screening, and give recommendation to anyone who doesn't have genetic engineering skill [14]. Democratization of hazardous knowledge significantly increase risk of bioweapon proliferation, as dangerous protocol become accessible to a broader audience.

- *Accidental Release of AI-Designed Pathogens*

  AI systems could unintentionally generate dangerous genetic modifications if not properly supervised. AI-designed pathogens, if accidentally released, could have catastrophic public health consequences. Historical biosecurity incidents, such as the Soviet smallpox outbreak in 1971, anthrax outbreak in 1979 and the UK's 2007 Foot and Mouth Disease virus leak, highlight the potential dangers of pathogen release from research facilities [15].

- Spread Genetically Modified Organism (GMO)

  The criminal release of GMO can cause diseases that have no known cure, spread quickly, and challenge the ability of health system to respond effectively. AI tool used to stimulate the spread of pandemic can also be used to spread of the pathogen [15].

- *AI powered Cyber-attack*

  AI-powered cyber tool can target critical biosecurity infrastructure such as BSL-3 and BSL-4 labs, through an automated attacks including phishing, malware, and system exploitation. These cyber-attack could lead to the release of dangerous biological and chemical agent by breaching containment protocol in research facilities. Customized AI-driven malware, like the "Occupy AI" LLM, can automate cyberattacks on biosecurity targets, raising the potential for bioterrorism via digital infiltration [16].

B. Vulnerabilities of AI-Driven Genetic Technology

AI-driven genetic technology presents multiple vulnerabilities that increase the risk of misuse and accidents:

- *Data Privacy and Security*

  Sharing genetic data globally enhances AI's accuracy but raises privacy concerns. If data security is compromised, it could enable malicious actors to misuse sensitive genomic information for targeted bioweapons [17].

- *Data quality and Bias.*

  AI models are only as good as the data they are trained on. If the training data is of poor quality or contains biases, this can lead to inaccurate or biased predictions. Misguided predictions could lead to harmful genetic modifications [18].

- *Transparency and explainability*

  AI models, especially complex machine-learning methods are often treated as black boxes, with their decision-making processes being difficult for humans to interpret. The "black box" nature of some AI models means researchers may not fully understand AI-driven genetic modifications, which could lead to unforeseen biosecurity risks [19].

- Cyber-security Risk.

  AI-driven genetic research relies heavily on digital infrastructure, making it vulnerable to cyber-attacks and target for malicious exploitation. Hackers could manipulate outputs to create dangerous pathogens or steal genomic data, enabling precision-targeted bioweapons.

LLM can allow malicious actors to gain access to dangerous information by manipulation prompt such as breaking up step or faking authority [20].

VI. CONCLUSION

The integration of AI with genetic engineering offers transformative benefits for human health, agriculture, and industry. However, these technologies also pose significant biosecurity risks, particularly due to the potential for malicious actors to misuse them. A comprehensive risk assessment reveals vulnerabilities that must be addressed through proactive mitigation strategies. By developing AI-specific biosecurity guidelines, increasing international collaboration, and implementing advanced monitoring systems, we can ensure that the benefits of AI-driven genetic engineering are not overshadowed by security risks.

For future work, this paper could expand its scope by exploring the ethical implications and regulatory frameworks required to govern the integration of AI in genetic engineering on a global scale. Further research could focus on developing real-time AI-based surveillance systems to detect biosecurity threats clearly and assess their efficacy in various scenarios, such as the accidental release of pathogens. Additionally, investigating the role of AI in facilitating targeted bioweapons and developing countermeasures to address emerging cyber threats in AI-driven genetic tools could provide valuable insights. A comparative analysis of international policies on AI and biotechnology biosecurity may also highlight gaps that need to be addressed for a more cohesive global response.

REFERENCES

[1] Carter, Sarah R. Wheeler, Nicole E. Chwalek, Sabrina. (2023). The Convergence of Artificial Intelligence and Life Science : Safeguarding Technology, Rethinking Governance, and Preventing Catastrophe. Nuclear Threat Initiative.

[2] Bhardwaj, A., Kishore, S., & Pandey, D. K. (2022). Artificial intelligence in biological sciences. *Life*, *12*(9), 1430.

[3] Grinbaum, A., & Adomaitis, L. (2024). Dual use concerns of generative AI and large language models. *Journal of Responsible Innovation*, *11*(1), 2304381.

[4] National Academies of Sciences, Engineering, and Medicine, Division on Earth and Life Studies, Board on Life Sciences, Board on Chemical Sciences and Technology, & Committee on Strategies for Identifying and Addressing Potential Biodefense Vulnerabilities Posed by Synthetic Biology. (2018). *Biodefense in the Age of Synthetic Biology*. National Academies Press (US).

[5] O'Brien, J. T., & Nelson, C. (2020). Assessing the risks posed by the convergence of artificial intelligence and biotechnology. *Health security*, *18*(3), 219-227.

[6] Sandbrink, J. B. (2023). Artificial intelligence and biological misuse: Differentiating risks of language models and biological design tools. *arXiv preprint arXiv:2306.13952*.

[7] De Haro, L. P. (2024). Biosecurity Risk Assessment for the Use of Artificial Intelligence in Synthetic Biology. *Applied Biosafety*.

[8] Prunckun, H. (2019). *Methods of inquiry for intelligence analysis*. Rowman & Littlefield.

[9] Lin, Z., Akin, H., Rao, R., Hie, B., Zhu, Z., Lu, W., Smetanin, N., Verkuil, R., Kabeli, O., Shmueli, Y., Dos Santos Costa, A., Fazel-Zarandi, M., Sercu, T., Candido, S., & Rives, A. (2023). Evolutionary-scale prediction of atomic-level protein structure with a language model. *Science (New York, N.Y.)*, *379*(6637), 1123–1130. https://doi.org/10.1126/science.ade2574

[10] Ruffolo, J. A., Nayfach, S., Gallagher, J., Bhatnagar, A., Beazer, J., Hussain, R., ... & Madani, A. (2024). Design of highly functional genome editors by modeling the universe of CRISPR-Cas sequences. *bioRxiv*, 2024-04.

[11] Shoham, D. China and Viruses: The Case of Dr. Xiangguo Qiu.

[12] Koblentz, G. D. (2017). The de novo synthesis of horsepox virus: implications for biosecurity and recommendations for preventing the reemergence of smallpox. *Health security*, *15*(6), 620-628.

[13] Urbina, F., Lentzos, F., Invernizzi, C., & Ekins, S. (2022). Dual Use of Artificial Intelligence-powered Drug Discovery. *Nature machine intelligence*, *4*(3), 189–191.

[14] Soice, E. H., Rocha, R., Cordova, K., Specter, M., & Esvelt, K. M. (2023). Can large language models democratize access to dual-use biotechnology?. *arXiv preprint arXiv:2306.03809*.

[15] Edwards, B. (2019). *Insecurity and Emerging Biotechnology: Governing Misuse Potential*. Springer.

[16] Usman, Y., Upadhyay, A., Gyawali, P., & Chataut, R. (2024). Is Generative AI the Next Tactical Cyber Weapon For Threat Actors? Unforeseen Implications of AI Generated Cyber Attacks. *arXiv preprint arXiv:2408.12806*.

[17] Ziller, A., Usynin, D., Braren, R., Makowski, M., Rueckert, D., & Kaissis, G. (2021). Medical imaging deep learning with differential privacy. *Scientific Reports*, *11*(1), 13524.

[18] Myllyaho, L., Raatikainen, M., Männistö, T., Mikkonen, T., & Nurminen, J. K. (2021). Systematic literature review of validation methods for AI systems. *Journal of Systems and Software*, *181*, 111050.

[19] Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature machine intelligence*, *1*(5), 206-215.

[20] Liu, Y., Deng, G., Xu, Z., Li, Y., Zheng, Y., Zhang, Y., ... & Liu, Y. (2023). Jailbreaking chatgpt via prompt engineering: An empirical study. *arXiv preprint arXiv:2305.13860*.