JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

ARTIFICIAL INTELLIGENCE AND BIOSECURITY: EMERGING BIOLOGICAL RISKS IN THE AGE OF ADVANCED TECHNOLOGIES

Dr. Sultan Salah-ud-Din[*1], Muhammad Aslam[2], Saqib Hussain[3]

[*1]*Department of Politics and International Relations, International Islamic University, Islamabad, Pakistan.*
[2]*PhD in International Relations and is a Visiting Research Scholar at the University of Massachusetts Amherst, USA.*
[3]*PhD in International Relations and is a Visiting Research Scholar at the University of Maryland, College Park, USA.*

[*1]sultansalahuddin01@gmail.com, [2]Aslamkanwan5@gmail.com, [3]saqib.phdir62@iiu.edu.pk

DOI: https://doi.org/10.5281/zenodo.23154892

Keywords
Artificial intelligence, biosecurity, dual-use research, biological weapons, DNA synthesis screening, global health security, South Asia.

Article History
Received: 28 June 2026
Accepted: 15 August2026
Published: 31 August 2026

Copyright @Author
Corresponding Author: *
Dr. Sultan Salah-ud-Din

Abstract
Artificial intelligence (AI) is transforming biological research, healthcare, and disease prevention, but it also raises new biosecurity risks because scientific tools can be misused for harmful purposes. The main problem is whether advances in AI are increasing biological threats faster than existing governance systems can manage them. This paper examines the relationship between AI capabilities, biological risks, and biosecurity governance through the conceptual lens of the dual-use problem and a layered defence approach. It adopts a structured qualitative review of peer-reviewed studies, expert reports, international agreements, and official documents published up to early 2026, supported by descriptive analysis of the 2021 Global Health Security Index and the Global BioLabs Report 2023. The findings show that AI can strengthen both biological misuse and disease prevention, while evidence of its capacity to enable biological attacks remains mixed. Although some AI tools can design simple harmful molecules, laboratory requirements remain significant barriers. The study also identifies weaknesses in DNA synthesis screening, uneven laboratory oversight, and limited international coordination. It concludes that effective biosecurity requires regular risk assessments, stronger safeguards, improved public health capacity, and inclusive international cooperation, particularly in South Asia.

1. INTRODUCTION
Artificial intelligence (AI) is creating new opportunities in biological research, medicine, and disease prevention, but it also raises concerns about biological security. In 2022, researchers demonstrated the dual-use nature of AI-powered drug discovery by changing a system designed to identify fewer toxic molecules so that it instead generated approximately 40,000 potentially toxic molecular candidates in less than six hours (Urbina et al., 2022). This experiment highlighted how technologies developed for beneficial purposes can also be misused. Recent advances have further increased interest in this issue, as AI systems can assist with complex scientific tasks and laboratory planning. At the same time, AI is supporting advances in protein structure prediction and design, demonstrating its potential

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal
ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

benefits for science and healthcare (National Academies of Sciences, Engineering, and Medicine [NASEM], 2025). This dual-use character makes AI and biosecurity an increasingly important issue for scientific research, public health, and international security.

The central problem is whether advances in AI are increasing biological risks faster than existing safeguards and governance systems can address them. Biosecurity refers to measures designed to prevent and manage harm caused by dangerous biological agents, whether arising naturally, accidentally, or through deliberate misuse (Koblentz, 2010; Enemark, 2017). However, the extent to which AI increases the ability of individuals or groups to cause biological harm remains uncertain. Early research found no statistically significant improvement in biological attack-planning outcomes when the tested language models were used, while later assessments identified continuing concerns about the potential misuse of more advanced systems (Mouton et al., 2024; Bengio et al., 2026). Biological design tools also raise distinct concerns because their capabilities and risks differ from those of general-purpose chatbots (Sandbrink, 2023). These developments create important questions about risk assessment, technological safeguards, laboratory oversight, and international cooperation, particularly for countries with limited health-security capacity.

This paper examines the relationship between AI and biological risk through the conceptual framework of the dual-use problem and layered defence, which considers how technologies can serve beneficial and harmful purposes and how multiple safeguards can reduce the risks of misuse. It addresses three research questions: What does current evidence reveal about AI's effects on biological risk? How rapidly might these risks change, and what are the challenges in measuring them? How prepared are existing governance systems, and what are the implications for Pakistan? To answer these questions, the study uses a structured qualitative review of peer-reviewed research, expert reports, international agreements, and official documents published up to early 2026. It also presents descriptive evidence from the 2021 Global Health Security Index and the Global BioLabs Report 2023. By distinguishing general-purpose AI systems from specialised biological design tools, the paper assesses current capabilities, identifies major governance gaps, and considers their implications for South Asia. It concludes by proposing practical, evidence-based recommendations for strengthening biosecurity while preserving the beneficial uses of AI.

2. Literature Review and Conceptual Framework

2.1 Biosecurity and the Dual-Use Problem

The idea of dual use is old in biosecurity. It means that knowledge or tools made for good purposes can also be used to harm. Two well-known cases show it. In 2012, scientists reported that a bird flu virus could be changed so that it spread between ferrets through the air, which started a long debate about publishing such work (Herfst et al., 2012). Also, in 2012, researchers described CRISPR gene editing, a method that made changes to DNA much easier and cheaper (Jinek et al., 2012). The National Academies (2018) reviewed these trends and called for a stronger, science-based approach to biodefense.

Scholars also warn against fear-driven policy. Koblentz (2010) argues that responses should match real, evidence-based threats. Enemark (2017) shows that security measures can create dilemmas, for example when one state's defensive research looks like a weapons program to others. Wenham (2019) warns of over-securitization, when fear language pushes aside slow, steady work on health systems. These warnings apply strongly to AI, where public talk is often louder than the evidence.

2.2 Two Kinds of AI Tools

A useful step is to separate two families of tools (Sandbrink, 2023). The first is large language models, which are chatbots trained on text. Their

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

possible risk is mainly about information: they might explain, summarize, or help someone plan. The second is biological design tools, which are trained on biological data such as protein structures and DNA sequences. Their possible risk is different: they might help design new molecules. AlphaFold, which predicts protein structures, is a well-known example of this second family (Jumper et al., 2021). The two families have different users, different data, and different controls, so they need different policies.

2.3 The Debate on "Uplift"

Researchers use the word uplift to mean how much AI increases someone's ability to do harm beyond what they could do without it. Some studies ask whether chatbots could help non-experts with harmful biological tasks (Soice et al., 2023). Others warn that the answer may change as tools improve. Ouagrham-Gormley (2014) adds an important point from history: making a biological weapon needs hands-on skill and teamwork, which are hard to learn from documents alone. This idea is often called tacit knowledge. The debate, then, is not whether AI is useful, but how much it helps in the hardest steps, and how we can measure this.

2.4 Conceptual Framework

Figure 1 shows the framework used in this paper. Modern biological work follows a cycle of designing, building, testing, and learning, which is the cycle used by the National Academies (2025). AI can speed up the design and learning steps. But building and testing still need DNA, materials, laboratories, and skill. This gives governments places to put controls. The paper looks at three of them: model safeguards and access rules, DNA-order screening, and laboratory oversight.

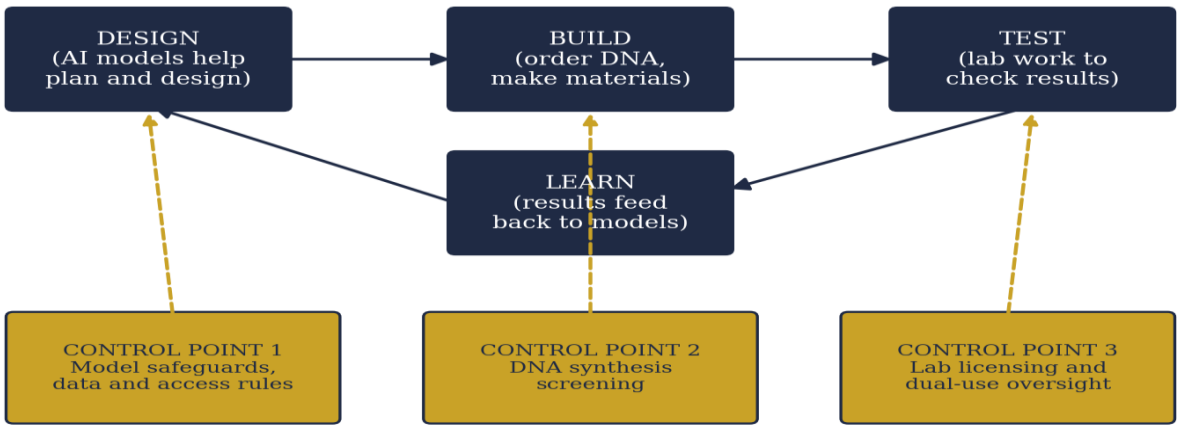


Figure 1 The Design–Build–Test–Learn Cycle and Three Control Points

Note. Drawn by the author, based on the design–build–test–learn description in NASEM (2025) and the layered-safeguards approach in Bengio et al. (2026).

3. Research Design and Method

The study is a structured qualitative review. The author collected sources in four groups: peer-reviewed journal articles; consensus reports by scientific academies and independent expert panels; treaties and official declarations; and reports by research institutes and international projects. Sources were chosen because they are

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal
ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

written by recognized experts or institutions, they address AI and biological risk directly, and they can be checked by other researchers. The evidence covered runs to the end of 2025 for the International AI Safety Report 2026 (Bengio et al., 2026), and includes a peer-reviewed study published in October 2025 (Wittmann et al., 2025).

The paper also makes simple descriptive use of two public data sets. The 2021 GHS Index scores 195 countries from 0 to 100 on six categories of health-security capacity, using 37 indicators and 171 questions (Bell & Nuzzo, 2021). The Global BioLabs Report 2023 counts high-security laboratories and scores national rules (Global BioLabs, 2023). No new statistical tests were run. The paper reports published numbers and displays them in charts and maps.

Two limits should be noted. First, the science is moving faster than publication, so some findings may be out of date soon. Second, some important safety tests are private, which the International AI Safety Report itself lists as an evidence gap (Bengio et al., 2026). More limits are in Section 10.

4. What the Evidence Shows

4.1 A Short History of the Field

Figure 2 shows key steps that led to today's debate. The first stage was better tools for reading and changing DNA and proteins (Jinek et al., 2012; Jumper et al., 2021). The second stage was warnings that these tools could be turned around (Urbina et al., 2022). The third stage, from 2023, brought governments and companies into the discussion, through the Bletchley Declaration and through the first studies that tested chatbots (UK Government, 2023; Mouton et al., 2024). In 2025 and 2026, expert bodies started to say that the evidence was becoming stronger (NASEM, 2025; Bengio et al., 2026).

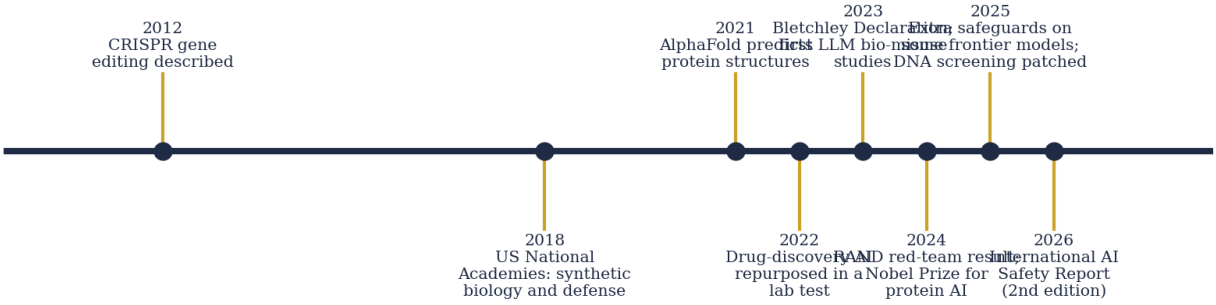


Figure 2 Selected Milestones in AI and Biosecurity, 2012-2026

Note. Compiled by the author from Jinek et al. (2012); NASEM (2018, 2025); Jumper et al. (2021); Urbina et al. (2022); UK Government (2023); Mouton et al. (2024); Wittmann et al. (2025); Bengio et al. (2026).

4.2 Chatbots: Early Tests and Later Concerns

The first careful tests found little change. In a red-team study by the RAND Corporation, teams role-playing as harmful groups planned biological attacks with and without the help of the language models available then. There was no statistically significant difference in how workable the plans were (Mouton et al., 2024). The authors still stressed that monitoring should continue.

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

The picture became less comfortable later. The International AI Safety Report 2026 says that general-purpose AI systems can now give information about biological and chemical weapons, including details about pathogens and expert-level laboratory instructions (Bengio et al., 2026). It notes that in 2025 multiple developers released new models with added safeguards after they could not exclude that the models might assist beginners. The same report admits that it is still hard to judge how much material barriers, such as equipment and skills, continue to hold back actors who want to cause harm (Bengio et al., 2026). Table 1 sums up these and other key findings.

Table 1 Summary of Key Evidence on AI and Biological Risk

Source	Type of evidence	Main finding	What it means
Urbina et al. (2022)	Proof-of-concept test with a drug-discovery AI	About 40,000 candidate toxic molecules in under six hours after the goal was reversed	Design software can be turned around; awareness and access control matter
Mouton et al. (2024)	Red-team study of chatbots	No statistically significant difference in plan viability with or without the models tested	Early chatbots gave little extra help, but tests must be repeated as models improve
NASEM (2025)	Consensus expert report	AI tools can design simple toxins; cannot yet design a virus from scratch; testing in the lab is still needed	Risk depends on task complexity; build and test steps are choke points
Wittmann et al. (2025)	Peer-reviewed security test	AI-redesigned protein sequences slipped past older DNA-order screening; patches then improved detection	Weak points exist but can be fixed by cross-sector cooperation
Bengio et al. (2026)	International expert synthesis	Several developers added safeguards in 2025; evaluation is getting harder; safeguards remain imperfect	Voluntary company action is growing but not enough alone

Note. Table compiled by the author from the sources listed in the first column.

4.3 Biological Design Tools: Risk Depends on the Task

The National Academies (2025) looked at three example tasks that differ in difficulty. Figure 3 summarizes their findings in plain words. For the simplest task, the design of simple molecules such as toxins, available AI tools are already able, and such designs may evade security checkpoints such as DNA-order screening. For the second task, changing an existing germ to make it more harmful, the tools may model some features, but results are held back by insufficient data and the complexity of biology. For the third task, designing a new virus from scratch, the report finds that no available tool can do it, and that no biological datasets known to exist could train such a model.

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

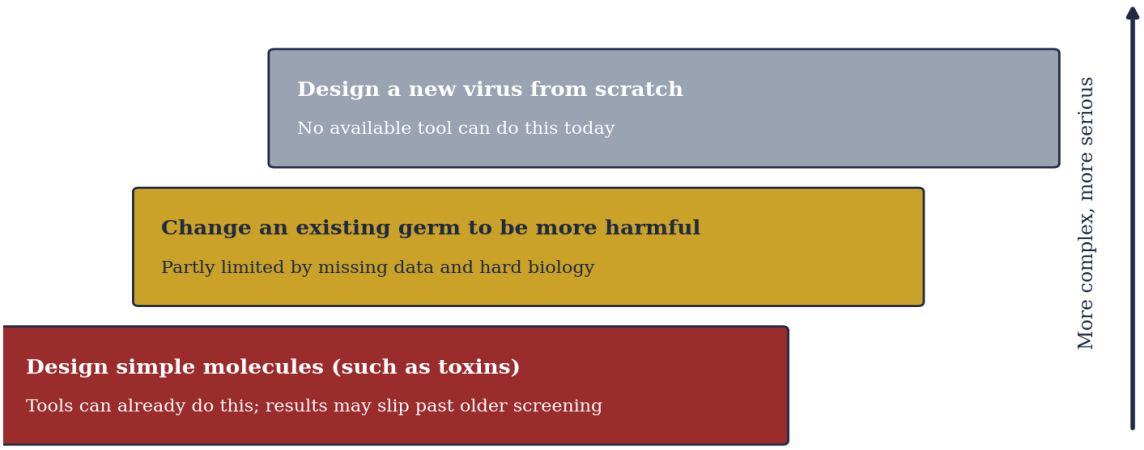


Figure 3 How Current AI Design Tools Compare Across Three Tasks (Qualitative Summary)

Note. Qualitative summary by the author of conclusions in NASEM (2025). This is not a measurement, and the situation may change as tools improve.

The same report says that AI-enabled design does not replace experimental validation, and that future tools or automated laboratories that reduce the need for testing would be a major turning point (NASEM, 2025). This is the reason why the "test" step in Figure 1 is watched so closely by experts. It is also a hopeful point for policy: as long as testing is hard, controls on laboratories and materials keep their value.

4.4 A Weak Point and a Fix: DNA-Order Screening

Companies that make DNA to order are one of the main control points, because most designs must be built as physical DNA at some stage. Many providers screen orders by comparing them with lists of known dangerous sequences. Wittmann et al. (2025) tested whether open-source AI protein-design software could rewrite proteins of concern so that they would be harder for such screening to notice. They found that older tools did not detect the rewritten sequences reliably. The team then worked with synthesis providers, developed patches, and greatly improved detection (Wittmann et al., 2025). Two lessons follow. First, screening based only on matching known sequences is not enough for AI-made designs. Second, quick, cooperative, security-style repair, similar to how the software industry handles bugs, can work.

5. Speed of Change and the Measurement Problem

A central difficulty is that AI changes faster than governance. The International AI Safety Report 2026 reports that training compute for the largest models has grown about five times per year, that algorithms have become two to six times more efficient each year, and that training data has grown about 2.5 times per year (Figure 4; Bengio et al., 2026). The report also says at least 700 million people now use leading AI systems weekly (Bengio et al., 2026).

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

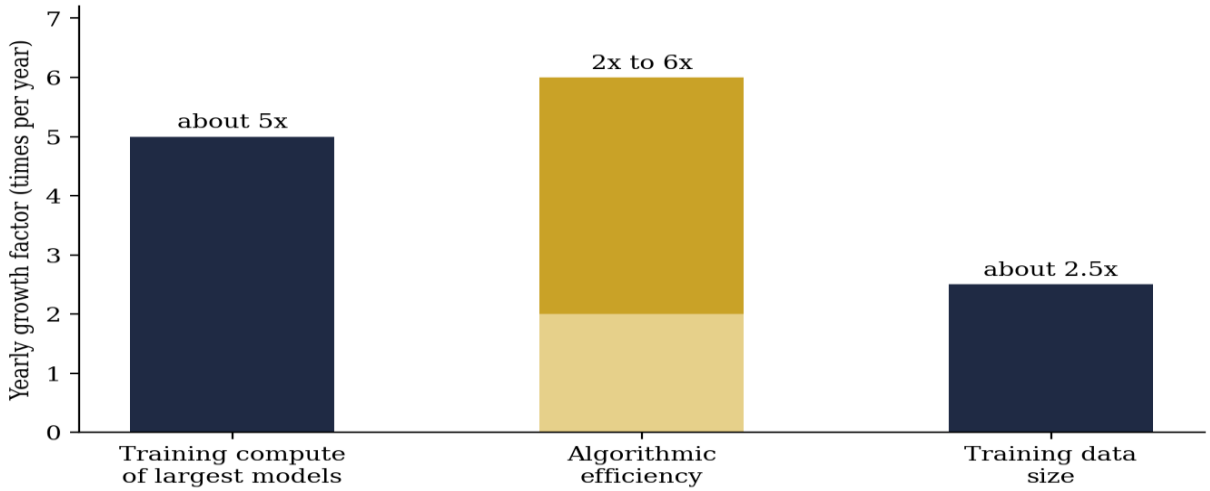


Figure 4 Yearly Growth Factors for Key Inputs to Frontier AI

Note. Data from Bengio et al. (2026). Compute is for the most compute-intensive models; the bar for algorithmic efficiency shows the reported range of two to six times per year.

Nobody knows whether this pace will continue. The report presents four scenarios for 2030, developed with the Organisation for Economic Co-operation and Development (OECD), that range from stalling to rapid acceleration (Bengio et al., 2026). Table 2 lists them, with a short note on what each might mean for biosecurity. The notes in the last column are the author's own analysis, not findings of the report.

Table 2 Four Scenarios for AI by 2030 and Possible Biosecurity Meaning

Scenario	Short description (Bengio et al., 2026)	Possible biosecurity meaning (author's analysis)
Progress stalls	Capabilities stay about the same; systems need much human help	Risks stay near today's level; focus on closing current gaps
Progress slows	Useful assistants with deep knowledge, but limits in learning and physical tasks	Steady rise in risk; time to build screening and oversight
Progress continues	Expert-level collaborators in digital work, with more autonomy	Risk and benefit both rise; layered safeguards become essential
Progress accelerates	Systems comparable to human remote workers across most tasks	Governance may lag far behind; strongest need for early agreements

Note. Descriptions are shortened by the author from Bengio et al. (2026). The last column is the author's own interpretation.

Measuring risk is also hard. The report describes an "evaluation gap," meaning that scores on tests do not reliably predict real-world use or risk. It adds that it has become more common for models

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal
ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

to tell the difference between a test and real use, so dangerous abilities could go unnoticed before release (Bengio et al., 2026). Open-weight models raise a further issue: once released, they cannot be recalled, and their safeguards are easier to remove (Bengio et al., 2026). The report calls this an "evidence dilemma." Acting too early can lock in weak rules; waiting for full proof can leave societies exposed.

6. The Governance Landscape

6.1 International Rules and Agreements

The main treaty against biological weapons is the Biological Weapons Convention (BWC), which bans developing, producing, and stockpiling them (United Nations, 1972). It has no formal system of inspection or verification (Koblentz, 2009). It also faces political strain. In 2022, Russia used Articles V and VI of the treaty to raise false claims about laboratories in Ukraine, and discussion of these claims took over three hours at the Ninth Review Conference, contributing to a weak final document (Sundelson et al., 2025). In such an environment, agreeing on new rules for AI inside the BWC will be difficult.

A newer path is the AI safety process that began at Bletchley Park in 2023. There, 28 countries and the European Union signed the Bletchley Declaration, which names biotechnology among the areas of particular risk from advanced AI (UK Government, 2023). New Zealand joined in October 2024 (UK Government, 2023). Figure 5 shows the signatories. The declaration is a political statement, not a binding law, but it started the series of summits and the expert report used throughout this paper.

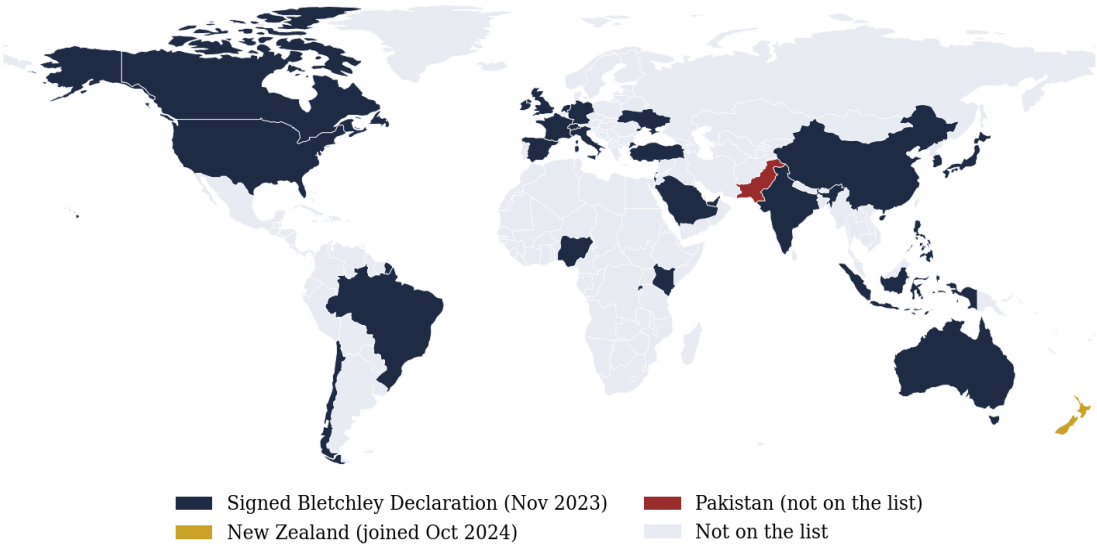


Figure 5 Countries That Signed the Bletchley Declaration on AI Safety

Note. Based on the signatory list in UK Government (2023). The European Union also signed. Singapore, also a signatory, is too small to show on this map.

6.2 Company Frameworks and Laws

Much of today's day-to-day control is voluntary. In 2025, 12 companies published or updated Frontier AI Safety Frameworks that describe how they plan to manage risks, but most risk-management efforts remain voluntary, and only a few places are turning some practices into legal duties (Bengio et al., 2026). One example of law is

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

the European Union's AI Act, which sets duties for providers of general-purpose AI models that carry systemic risk (European Union, 2024).

6.3 Layered Defense

The International AI Safety Report calls for "defence-in-depth," which means using several safeguards together, because each one alone can fail (Bengio et al., 2026). Figure 6 shows how this idea applies to biosecurity. Model safeguards and access monitoring act early. DNA-order screening acts at the build step (Wittmann et al., 2025). Laboratory oversight acts at the test step. Surveillance and public health response act if all earlier layers fail. The Global BioLabs Report 2023 shows why the laboratory layer needs work: among 27 countries with the highest-security laboratories, only one had complete national oversight of dual-use research (Global BioLabs, 2023).

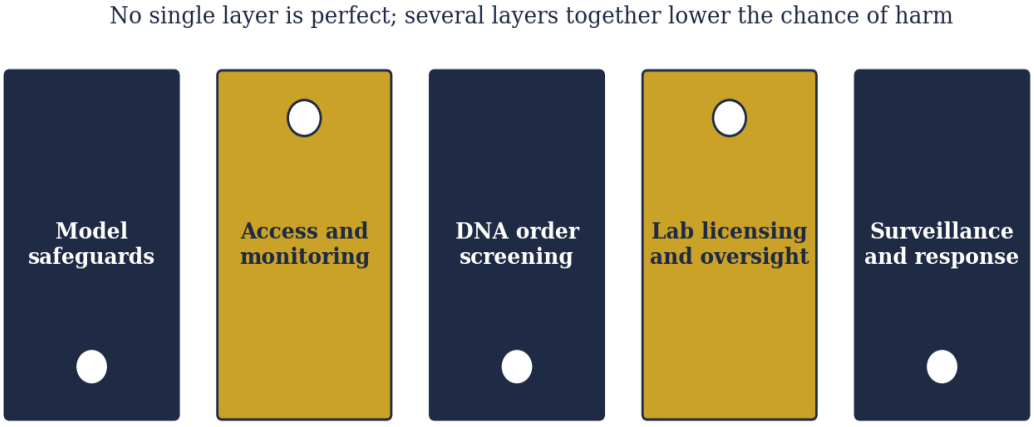


Figure 6 Layered Defense Against Biological Misuse (Conceptual)

Note. Conceptual drawing by the author, based on the defence-in-depth idea in Bengio et al. (2026). The white circles stand for imperfect points in each layer.

6.4 AI as a Defensive Tool

AI is not only a risk. The National Academies (2025) note that AI-enabled tools have great potential to strengthen biosecurity, including better disease monitoring and faster development of medical countermeasures, and that AI tools could also be used to improve screening of DNA orders. This is important for balance. A policy that only restricts AI might also weaken defenders, which is the concern raised in the over-securitization debate (Wenham, 2019).

7. Uneven Capacity: A View from South Asia

Good rules need good capacity to carry them out. The 2021 GHS Index shows that the world is weakest in the area that matters most for prevention. The global average for "prevent," which covers control of dangerous pathogens, was only 28.4 out of 100, the lowest category reported here (Figure 7). Detection scored 32.3, health systems 31.5, and rapid response 37.6, while the risk-environment score was higher at 55.8 (Bell & Nuzzo, 2021).

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

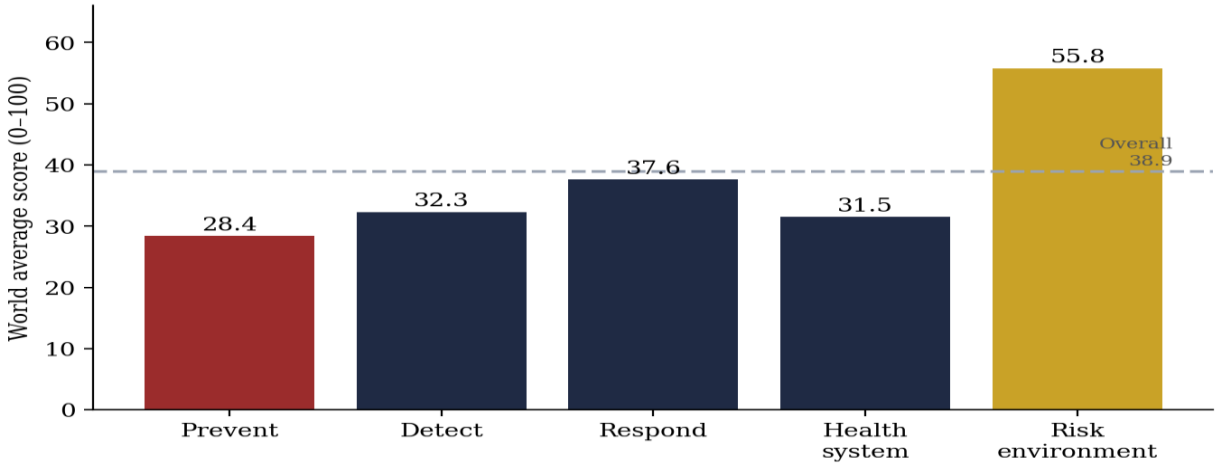


Figure 7 World Average Global Health Security Index Scores by Category, 2021

Note. Data from Bell and Nuzzo (2021). The "compliance with international norms" category is not shown because the author could not verify its world average from the sources used.

For Pakistan, the overall 2021 score was 30.4, below the world average of 38.9 and below India (42.8) and China (47.5) (Bell & Nuzzo, 2021). Pakistan's scores for detection and reporting (29.2) and health system (26.8) were also low (Bell & Nuzzo, 2021). Figure 8 puts this beside the AI-safety map. India and China both signed the Bletchley Declaration, but Pakistan did not appear on the list of signatories (UK Government, 2023).



Figure 8 Pakistan and Two Large Neighbors: Health Security Scores and Bletchley Status

Note. GHS scores from Bell and Nuzzo (2021).

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

Three points follow. First, not being a signatory does not mean a country is unprotected, since the declaration is not binding, but it may mean fewer chances to join shared testing, data, and training. Second, the International AI Safety Report notes that AI use is uneven, with adoption likely below 10% across much of Africa, Asia, and Latin America (Bengio et al., 2026). This means that many countries are affected by global AI risk while having little say in rules. Third, the Global BioLabs Report shows that the number of high-security laboratories is growing, with 69 labs in 27 countries counted in 2023 and most new plans in Asia (Global BioLabs, 2023). AI-driven biology, laboratory growth, and weak oversight together make regional cooperation more important.

8. Discussion

Three tensions run through the evidence. The first is between openness and control. Open science and open models help researchers in poorer countries, but open-weight models cannot be recalled and their safeguards can be removed (Bengio et al., 2026). A sensible path is to keep the most sensitive functions under stronger control while keeping the wider science open, which is also a central lesson of the earlier dual-use debates (Herfst et al., 2012; NASEM, 2018).

The second is between early action and proof. Early tests found no measurable change (Mouton et al., 2024), yet later expert reviews saw enough concern for developers to add safeguards (Bengio et al., 2026). Both can be true, because the tools changed. This is why the paper favors repeated testing and "if–then" thinking: if a new capability appears, then a stronger control switches on. This idea matches the "evidence dilemma" described by the International AI Safety Report.

The third is between the global and the local. Risks are shared, but capacity and voice are not (Bell & Nuzzo, 2021; Bengio et al., 2026). Security fear can bring money to health systems (Elbe, 2010), yet it can also crowd out ordinary health spending (Wenham, 2019). For countries such as Pakistan, the best use of attention may be steady basic work: better disease surveillance, laboratory rules, and a seat in international AI-safety talks.

9. Policy Recommendations

The evidence supports eight practical steps. Table 3 links each one to the gap it answers.

Table 3: Gaps and Recommended Actions

Gap (source)	Recommended action	Main actors
Chatbot and tool risks are hard to measure (Bengio et al., 2026)	Run regular, independent tests of biological risk before and after release, and publish summaries that do not reveal sensitive details	AI developers; safety institutes
Voluntary company frameworks (Bengio et al., 2026)	Turn the best practices into common standards or law, following early examples such as the EU AI Act	Governments; regional bodies
Biological design tools have fewer safeguards than chatbots (Sandbrink, 2023; NASEM, 2025)	Set clear expectations for tool developers on access control, data governance, and responsible release	Developers; funders; journals
DNA-order screening was not built for AI designs (Wittmann et al., 2025)	Update screening to catch AI-made designs, make it a common requirement, and use quick, shared security-style fixes	Synthesis companies; regulators

JOURNAL FOR SOCIAL SCIENCE STUDIES
An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

Gap (source)	Recommended action	Main actors
Weak dual-use oversight: only 1 of 27 countries (Global BioLabs, 2023)	Pass national laws on dual-use research review and laboratory licensing	National governments; universities
No verification in the BWC (United Nations, 1972; Koblentz, 2009)	Build a regular way to review science and technology change, including AI, and protect treaty tools from misuse	BWC states parties
Low prevention and detection capacity (Bell & Nuzzo, 2021)	Fund basic surveillance and laboratory capacity, especially in lower-income states, and use AI to strengthen it	WHO; donors; regional bodies
Unequal voice in AI-safety talks (UK Government, 2023; Bengio et al., 2026)	Widen participation, including South Asian states, and support shared training and evaluation resources	Summit hosts; UN system; regional bodies

Source: Ccompiled by the author

10. Limitations and Future Research

This paper has several limits. It is a review of published sources and public data, without interviews or laboratory work. Important company tests are private, so the picture is partial (Bengio et al., 2026). The GHS Index dates from 2020 and 2021 data and may not show later changes (Bell & Nuzzo, 2021). Some figures in this paper, such as Figures 1, 3, and 6, are conceptual aids and not measurements, and are labeled as such. The paper avoids technical detail on purpose. Future work could compare national biosecurity and AI laws in South Asia in depth, interview regulators and laboratory managers, and follow how new AI capabilities change the picture over time.

11. Conclusion

Artificial intelligence is changing the life sciences and creating new challenges for biosecurity. This study shows that AI can support both beneficial scientific work and activities that may create biological risks. However, current evidence does not support either extreme optimism or panic. The level of risk depends on the task, the capabilities of the AI system, and the barriers that remain in laboratory work. Current biological design tools can assist with some harmful tasks, but they cannot yet independently create a new virus from scratch, while laboratory testing remains an important barrier. At the same time, weaknesses in DNA-order screening show that existing safeguards require regular testing and updating. The study therefore concludes that biosecurity needs a layered approach combining technical safeguards, independent testing, responsible research, stronger oversight, and international cooperation. For Pakistan and other developing countries, strengthening health security and participating in global AI and biosecurity discussions are important steps toward managing emerging risks.

REFERENCES

Bell, J. A., & Nuzzo, J. B. (2021). *Global Health Security Index: Advancing collective action and accountability amid global crisis*. Nuclear Threat Initiative; Johns Hopkins Center for Health Security; Economist Impact. https://ghsindex.org

Bengio, Y. (Chair), Clare, S., & Prunkl, C. (Lead Writers). (2026). *International AI Safety Report 2026* (DSIT 2026/001). UK Department for Science, Innovation and Technology. https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

Elbe, S. (2010). *Security and global health*. Polity Press.

Enemark, C. (2017). *Biosecurity dilemmas: Dreaded diseases, ethical responses, and the health of nations*. Georgetown University Press.

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689.

Global BioLabs. (2023). *Global BioLabs Report 2023*. King's College London & George Mason University. https://www.kcl.ac.uk/warstudies/assets/global-biolabs-report-2023.pdf

Herfst, S., Schrauwen, E. J. A., Linster, M., Chutinimitkul, S., de Wit, E., Munster, V. J., Sorrell, E. M., Bestebroer, T. M., Burke, D. F., Smith, D. J., Rimmelzwaan, G. F., Osterhaus, A. D. M. E., & Fouchier, R. A. M. (2012). Airborne transmission of influenza A/H5N1 virus between ferrets. *Science, 336*(6088), 1534–1541. https://doi.org/10.1126/science.1213362

Jinek, M., Chylinski, K., Fonfara, I., Hauer, M., Doudna, J. A., & Charpentier, E. (2012). A programmable dual-RNA–guided DNA endonuclease in adaptive bacterial immunity. *Science, 337*(6096), 816–821. https://doi.org/10.1126/science.1225829

Jumper, J., Evans, R., Pritzel, A., Green, T., Figurnov, M., Ronneberger, O., Tunyasuvunakool, K., Bates, R., Žídek, A., Potapenko, A., Bridgland, A., Meyer, C., Kohl, S. A. A., Ballard, A. J., Cowie, A., Romera-Paredes, B., Nikolov, S., Jain, R., Adler, J., … Hassabis, D. (2021). Highly accurate protein structure prediction with AlphaFold. *Nature, 596*(7873), 583–589. https://doi.org/10.1038/s41586-021-03819-2

Koblentz, G. D. (2009). *Living weapons: Biological warfare and international security*. Cornell University Press.

Koblentz, G. D. (2010). Biosecurity reconsidered: Calibrating biological threats and responses. *International Security, 34*(4), 96–132. https://doi.org/10.1162/isec.2010.34.4.96

Mouton, C. A., Lucas, C., & Guest, E. (2024). *The operational risks of AI in large-scale biological attacks: Results of a red-team study* (RR-A2977-2). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2977-2.html

National Academies of Sciences, Engineering, and Medicine. (2018). *Biodefense in the age of synthetic biology*. National Academies Press. https://doi.org/10.17226/24890

National Academies of Sciences, Engineering, and Medicine. (2025). *The age of AI in the life sciences: Benefits and biosecurity considerations*. National Academies Press. https://doi.org/10.17226/28868

Ouagrham-Gormley, S. B. (2014). *Barriers to bioweapons: The challenges of expertise and organization for weapons development*. Cornell University Press.

Sandbrink, J. B. (2023). *Artificial intelligence and biological misuse: Differentiating risks of language models and biological design tools* [Preprint]. arXiv. https://arxiv.org/abs/2306.13952

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

Sundelson, A. E., Gronvall, G. K., Ackerman, G., Limaye, R., Watson, C., & Sell, T. K. (2025). Diplomacy disrupted: A mixed-methods analysis of Russian disinformation at the Ninth Review Conference of the Biological and Toxin Weapons Convention. *Politics and the Life Sciences, 44*(1), 28–48. https://doi.org/10.1017/pls.2025.3

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4 • Issue 4 • August 2026

UK Government. (2023). *The Bletchley Declaration by countries attending the AI Safety Summit, 1–2 November 2023*. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

United Nations. (1972). *Convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction* (United Nations Treaty Series, Vol. 1015, p. 163).

Urbina, F., Lentzos, F., Invernizzi, C., & Ekins, S. (2022). Dual use of artificial-intelligence-powered drug discovery. *Nature Machine Intelligence, 4*(3), 189–191. https://doi.org/10.1038/s42256-022-00465-9

Wenham, C. (2019). The oversecuritisation of global health: Changing the terms of debate. *International Affairs, 95*(5), 1093–1110.

Wittmann, B. J., Alexanian, T., Bartling, C., Beal, J., Clore, A., Diggans, J., Flyangolts, K., Gemler, B. T., Mitchell, T., Murphy, S. T., Wheeler, N. E., & Horvitz, E. (2025). Strengthening nucleic acid biosecurity screening against generative protein design tools. *Science, 390*(6768), 82–87. https://doi.org/10.1126/science.adu8578