

Geopolitical Report ISSN 2532-845X



Special Eurasia
Geopolitical Intelligence & Risk Assessment



GENERATIVE AI, CRISPR, AND EMERGING BIO-SECURITY THREATS

Volume 1

APRIL 2026

Geopolitical Report

Publisher: SpecialEurasia

In the first volume of Geopolitical Report ISSN 2532-845X titled *Generative AI, CRISPR, and Emerging Bio-Security Threats* SpecialEurasia OSINT Team aims at analysing the geopolitical implication for national security of use of Generative AI in the field of biotechnology.

Website: www.specialeurasia.com

Email: info@specialeurasia.com

Online ISSN: **2532-845X**

Date: **April 2026**

Editors: **Giuliano Bifulchi, Silvia Boltuc**

Scope

SpecialEurasia is a consulting and media agency specialising in geopolitical intelligence and risk assessment. We empower businesses, government agencies, and organisations with the critical insights needed to navigate today's rapidly evolving geopolitical landscape. Our expertise spans from strategic intelligence and risk analysis to media reporting and specialised training, ensuring our clients stay ahead of emerging challenges and seize new opportunities.

SpecialEurasia's publication, *Geopolitical Report ISSN 2532-845X*, aims at investigating the current geopolitical and socio-cultural events and trends which are shaping the world of international relations, business and security creating a debate by allowing scholars and professional experts to share their views, perspectives, work results, reports and research findings. One can submit manuscripts, analytical reports, critical responses, short articles, commentaries, book reviews to info@specialeurasia.com

Copyright © 2026 SpecialEurasia

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at info@specialeurasia.org.

Tables of Contents

Abstract	5
Introduction	6
Threat Vector Analysis	7
Strategic Foresight and Early Warning.....	10
Policy and Defence Architecture.....	12
References	15

Abstract

This report investigates the crucial intersection of generative artificial intelligence (AI) and CRISPR gene-editing technology, a combination presently reshaping international biosecurity. With the digitalisation and automation of biological design, conventional biosecurity frameworks, which rely on physical containment and material controls, are losing their efficacy. The report delineates four principal threat vectors: cyber incursions into biotechnology facilities, extremist simulation of genetic constructs, organized criminal misappropriation of synthetic materials, and state-sponsored grey zone operations.

A primary concern among these risks is generative AI's ability to reduce technical prerequisites, allowing individuals with minimal scientific expertise to undertake intricate biological design projects with exceptional celerity. To address these developing hazards, the study recommends adopting a "cyberbiosecurity" approach, conceptualising the safeguarding of digital systems as intrinsically linked to biological security. The proposed policy interventions comprise implementing risk-based regulatory structures for biological AI models, unifying foundational cybersecurity measures in bio-foundries and laboratories, and establishing regional, cross-sectoral intelligence-sharing networks. Ultimately, the paper contends that the global security environment of the next ten years will be determined by the efficacy of governing bodies in synthesising cyber, biological, and behavioural intelligence into a proactive early warning system designed to identify threats before they emerge in the physical realm.

Introduction

The quick integration of AI and innovative biotechnology is altering global security in ways that existing defence strategies are not yet equipped to handle. In the last ten years, generative AI has transformed from an experimental computing tool into a powerful system for various biological applications, including modelling protein structures, forecasting gene interactions, and producing genetic sequences efficiently and on a large scale. These systems, initially created to stimulate advancements in biomedicine, now enhance capabilities throughout the biotechnology sector. Their integration with gene-editing platforms such as CRISPR has created a new strategic environment in which biological design is increasingly digital, automated, and accessible. This transition offers significant advancements for both medicine and public health, yet it concurrently poses a critical dual-use challenge requiring immediate policy consideration.

Generative artificial intelligence comprises machine learning models that can create original content, such as text, imagery, molecular configurations, or genetic sequences, by leveraging patterns identified in extensive data collections. These models are instrumental in the biosciences, enabling the proposal of protein designs, the optimisation of CRISPR guide RNAs, and the simulation of biological pathways with a swiftness and accuracy that significantly surpass human abilities. Recent studies highlight such tools can significantly reduce the expertise required to perform complex biological design tasks, effectively lowering the barrier to entry for actors with limited scientific training.¹

CRISPR is a gene-editing technique that allows precise changes to DNA within living organisms. Its programmability, efficiency, and low cost have made it the dominant platform for genetic engineering across research, agriculture, and therapeutic development. CRISPR's transformative potential is widely recognised, but its

¹ Zaixi Zhang et al., «Generative AI for Biosciences: Emerging Threats and Roadmap to Biosecurity», arXiv, novembre 4, 2025, <http://arxiv.org/abs/2510.15975>.

accessibility also raises concerns about misuse, particularly when combined with AI-driven design systems that can advance experimentation and reduce trial-and-error cycles.²

In this scenario, biosecurity comprises the protocols, methodologies, and operational procedures implemented to avert the inappropriate utilisation of biological agents, genetic engineering technologies, and related digital infrastructures. Historically, biosecurity frameworks have focused on physical pathogens, laboratory containment, and material controls. However, the integration of digital technologies into biology, spearheaded by AI, cloud-powered genomic repositories, and automated laboratory equipment, has increased the attack surface beyond its customary confines. Analysts' current projections indicate an increasing trend of biological risks emerging from locations other than traditional wet laboratories. These threats are now recognised as originating from cyber domains, the manipulation of data, and AI-powered design pipelines.³

The convergence of generative AI and CRISPR concurrently elevates the risk of exploitation by non-state actors, rogue entities, or asymmetric adversaries. The effectiveness with which governments and institutions change their security structures to address this evolving, digitally driven biological threat landscape will define the next ten years.

Threat Vector Analysis

The intersection of generative artificial intelligence and CRISPR is altering the landscape of threats, increasing the velocity, scope, and ease of biological engineering. AI serves as an accelerant for threats by reducing the time, expertise, and resources historically needed

² Michael Ben Okon et al., «From pandemics to preparedness: harnessing AI, CRISPR, and synthetic biology to counter biosecurity threats», *Frontiers in Public Health*, vol. 13, novembre 2025, <https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1711344/full>.

³ Renan Chaves de Lima, Juarez Antonio Simões Quaresma, «Emerging technologies transforming the future of global biosecurity», *Frontiers in Digital Health*, vol. 7, giugno 2025, <https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2025.1622123/full>.

to conceptualise and model biological systems. Expert analyses of synthetic biology and AI integration uniformly conclude that AI lowers technical impediments, distributes capabilities, and renders biosecurity threats less concentrated and more elusive. This transition elevates the probability that malicious entities, including non-state actors, criminal organisations, or ideologically driven individuals, may leverage biotechnological advancements beyond the scope of state-sponsored initiatives.

In the near term (three to five years), several asymmetric threat vectors become more plausible. A significant and increasing concern is the incidence of cyber intrusions into biotechnology facilities. Contemporary laboratory settings depend on cloud-connected sequencing platforms, automated bio-foundries, and digital CRISPR design tools. Evidence suggests that cybersecurity weaknesses in biosecurity could enable malicious actors to alter experimental results, impede supply chains, or undermine DNA synthesis verification. The execution of such attacks would not require specialised biological knowledge, as they exploit deficiencies in digital infrastructure to precipitate extensive biological outcomes.⁴

Additionally, artificial intelligence-driven design tools may indirectly enhance terrorist proclivity for biological agents. Research shows that despite considerable challenges posed by tacit knowledge and laboratory constraints, AI may prove instrumental in modelling genetic constructs or predicting functional characteristics. There are warnings that this support could reduce the conceptual obstacles for extremist factions looking to intimidate governmental bodies or civilian populations. While these tools do not offer immediate, ready-to-use solutions, they can accelerate comprehension, shorten the

⁴ Asha M. George, «The National Security Implications of Cyberbiosecurity», *Frontiers in Bioengineering and Biotechnology*, vol. 7, marzo 2019, <https://www.frontiersin.org/journals/bioengineering-and-biotechnology/articles/10.3389/fbioe.2019.00051/full>; «Cyberbiosecurity and Espionage», *Cyberbiosecurity*, 2022, https://www.cyberbiosecurity.ch/Espionage_Cyberbiosecurity.html; Dr Rafael J. Gomez, «Cyberbiosecurity: The New Frontier of Protection», *Journal of Bioterrorism & Biodefense*, vol. 16, fasc. 6, 2025, pp. 1–4.

process of experimentation, and bolster narratives promoting the idea of self-made biological dangers.⁵

An additional consideration is the potential for organised crime networks to perceive biotechnology as a high-yield domain within the black market. The illicit trade in synthetic drugs provides evidence of how criminal organisations leverage chemical synthesis and international supply chains. As AI-enabled biological design becomes more accessible, there is a credible risk that criminal organisations could attempt to monetise genetically modified materials, circumvent regulatory controls, or exploit compromised DNA synthesis providers. The risk is not only associated with constructed pathogens, but includes fraudulent biological commodities, corrupted genetic details, and unapproved gene-editing facilities.⁶

Ultimately, state-aligned actors in the grey zone possess the capability to leverage the confluence of AI and CRISPR for the execution of deniable operations that fall short of armed conflict. This could encompass cyber-enabled disruptions to vaccine development, the dissemination of targeted misinformation regarding gene editing, or clandestine interference with regional bio-manufacturing capabilities. The distributed architecture of AI-driven biotechnology complicates attribution, enhancing the strategic attractiveness of such endeavours.⁷

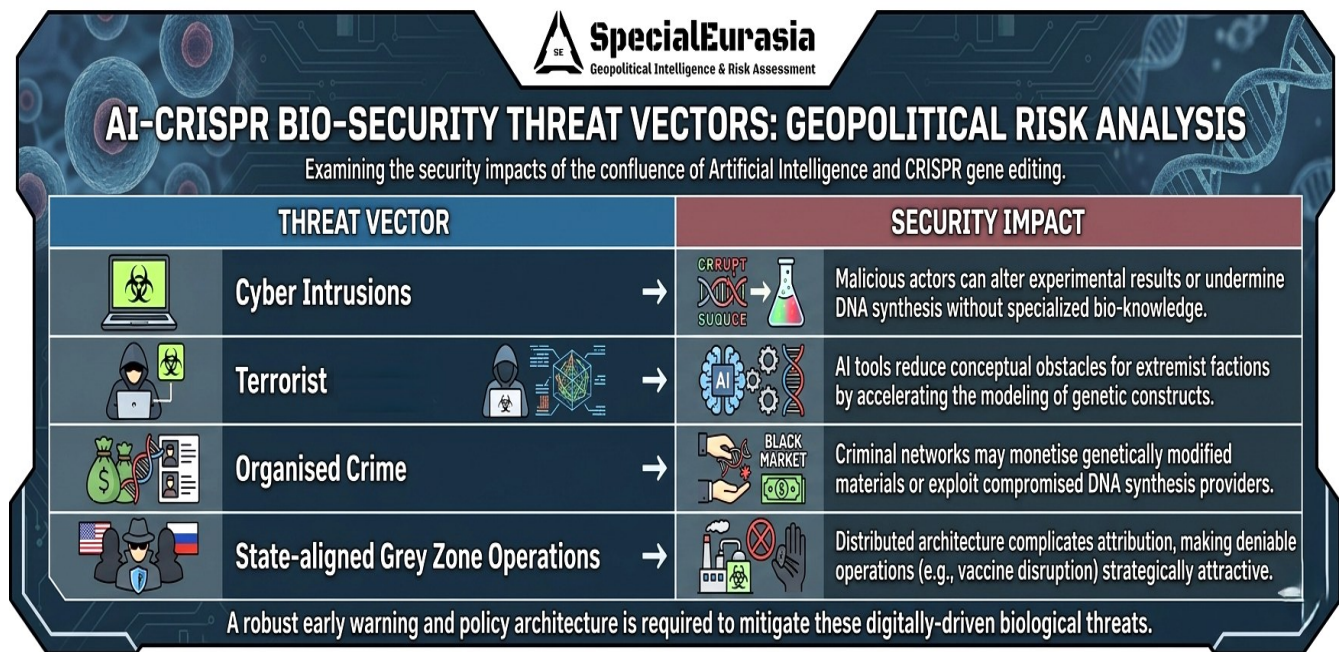
Cumulatively, these vectors illustrate AI's dual effect of augmenting existing vulnerabilities and generating unprecedented opportunities for illicit application. The threat environment is no longer defined solely by physical access to pathogens but by the

⁵ National Academies of Sciences, Engineering, and Medicine, «Biotechnology in the Age of Synthetic Biology», *Biodefense in the Age of Synthetic Biology*, Washington D.C., The National Academic Press, 2018, <https://www.nationalacademies.org/read/24890/chapter/1>, pp. 15–22; D.R.J. Gomez, *op.cit.*

⁶ Zainab Asimiyu, *AIDriven Biothreats: Emerging Risks and Countermeasures*, 2025, https://www.researchgate.net/publication/389148605_AIDriven_Biothreats_Emerging_Risks_and_Countermeasures.

⁷ Thom Dixon, «The grey zone of cyber-biological security», *International Affairs*, vol. 97, fasc. 3, maggio 2021, pp. 685–702.

intersection of digital systems, biological design tools, and adversaries willing to exploit both.



Strategic Foresight and Early Warning

The confluence of generative artificial intelligence and CRISPR technology requires a recalibration of conventional early warning systems, which traditionally rely on biological agents, laboratory surveillance, and epidemiological data. The evolving nature of threats is significantly influenced by digital advancements such as AI-powered design tools, cloud-based genomic platforms, and automated laboratory systems. These technologies operate at a pace that surpasses traditional monitoring mechanisms. Strategic foresight must therefore integrate biological, digital, and behavioural intelligence streams to detect threats that may originate in cyberspace long before they manifest in the physical domain. Enhanced digital biological situational awareness constitutes the foundation of a credible early warning architecture. AI-powered biotechnology generates subtle indicators of biological risk, such as anomalous sequence design activity, atypical patterns in DNA synthesis orders, or irregular access to CRISPR design platforms. Detection of these signals requires integrated monitoring systems that synthesise cyber threat intelligence

and biosecurity analytics. Regional authorities will need the capacity to monitor irregularities in biological data streams, detect unauthorised modifications within genomic databases, and identify efforts to circumvent DNA synthesis screening procedures.⁸

The inclusion of AI-assisted anomaly detection within early warning systems is essential. Machine learning models offer a means to support the identification of anomalous patterns across laboratory automation logs, cloud-based bioinformatics pipelines, and supply chain telemetry. The domain of digital health security research shows that artificial intelligence possesses the capability to identify anomalies in sequencing processes or the operation of laboratory robotics, which could signify cyber intrusions or data tampering. These tools do not replace human analysts but augment their ability to detect weak signals that would otherwise remain obscured.⁹

Establishing cross-sectoral intelligence sharing frameworks is crucial for a resilient early warning system. Academic laboratories, private bio-foundries, pharmaceutical companies, and cloud service providers all contribute to the highly fragmented nature of the biotechnology sector. Academic literature stresses that no single actor possesses a complete picture of emerging risks. Regional early warning networks need to incorporate information from public health agencies, cybersecurity centres, DNA synthesis providers, and AI model developers. This includes establishing secure channels for reporting anomalous biological activity, cyber incidents affecting laboratory infrastructure, and suspicious attempts to access high-risk AI tools.

In conclusion, strategic foresight entails the consideration of both geopolitical and behavioural indicators. Adversaries might show their intentions via online discussions, acquisition behaviours, or synchronised influence operations focused on biotechnology

⁸ Mariam Elgabry, Shane Johnson, «Cyber-biological convergence: a systematic review and future outlook», *Frontiers in Bioengineering and Biotechnology*, vol. 12, fasc. 1456354, 2024, <https://pmc.ncbi.nlm.nih.gov/articles/PMC11458441/>.

⁹ Engineering National Academies of Sciences et al., «Promoting and Protecting AI-Enabled Innovation for Biosecurity», *The Age of AI in the Life Sciences: Benefits and Biosecurity Considerations*, National Academies Press (US), 2025, <https://www.ncbi.nlm.nih.gov/books/NBK614605/>.

narratives. Monitoring these signals can provide early insight into emerging threat trajectories, particularly when combined with technical indicators from digital and biological systems.¹⁰

In conclusion, a robust early warning system designed to detect AI-driven biological threats requires multifaceted integration of cyber intelligence, biological monitoring, AI-powered analytical capabilities, and collaborative information sharing across various sectors. The rapid advancement and opacity of AI-driven biotechnology require a pre-emptive, intelligence-focused strategy to identify threats prior to their materialisation from digital schematics into biological forms.

Policy and Defence Architecture

The increasing integration of generative AI and CRISPR demands a defensive framework characterised by foresight over responsiveness. Current biosecurity strategies, which focus on lab containment, pathogen identification, and physical security, are inadequate given that biological threats can now emerge from digital alterations, AI-driven design, or compromised cloud systems. The following policy measures represent actionable strategies that governments and regional blocs can implement to strengthen resilience against digitally accelerated biological threats.

1. Establish a risk-tiered regulatory framework for biological AI models.

Governments should implement a risk-based tiered governance framework for AI systems employed in biological design, analogous to nascent structures being suggested within academic discourse and global policy dialogues.¹¹ This approach would classify AI tools according to their capability, misuse potential, and access requirements. Systems that pose a high risk, such as those capable of generating

¹⁰ Andraz Kastelic, Louison Mazeaud, «Cyberbiosecurity: A Matter of International Peace and Security?», 2025, <https://unidir.org/publication/cyberbiosecurity-a-matter-of-international-peace-and-security/>.

¹¹ Mengdi Wang et al., «A call for built-in biosecurity safeguards for generative AI tools», *Nature Biotechnology*, vol. 43, fasc. 6, giugno 2025, pp. 845–847.

functional genetic constructs, optimising CRISPR edits, or predicting protein interactions, necessitate mandatory safeguards. Such a framework would not impede legitimate research but would create a structured mechanism to prevent misuse while maintaining scientific progress.

2. Strengthen cyberbiosecurity standards across the biotechnology sector.

Considering the growing dependence on cloud-connected sequencing platforms, automated laboratories, and digital CRISPR design tools, cyberbiosecurity must be integrated into national defence strategies. Academic analyses consistently highlight that cyber intrusions into biological systems can produce real-world biological consequences, making cybersecurity inseparable from biosecurity. Governmental bodies should institute foundational cybersecurity protocols for laboratories, DNA synthesis entities, and bio-foundries. This necessitates continuous monitoring of cloud-based genomic platforms, validation of CRISPR design processes and laboratory automation logs, and obligatory reporting of cyber incidents affecting biological infrastructure. This approach mirrors the protection principles applied to other forms of critical infrastructure, recognising biotechnology as a strategic asset increasingly exposed to digital compromise..

3. Establish regional intelligence-sharing networks for AI-accelerated biological threats.

No single institution possesses the requisite visibility to identify nascent biological threats facilitated by artificial intelligence; early detection needs the fusion of intelligence across sectors, integrating data from public health organisations, cybersecurity entities, DNA synthesis firms, and AI model creators. Governing bodies should establish regional early warning networks to facilitate the real-time dissemination of information concerning anomalous biological activities, collaborative assessment of cyber incidents, unified supervision of DNA synthesis screening, and synchronised reactions to developing indicators. These networks might replicate current counterterrorism and cyber intelligence structures, with

modifications to identify digital indicators of biological threats, establishing a contemporary defence framework prepared for the dual-use challenges presented by generative AI and CRISPR.

References

- Asimiyu, Zainab, *AI-Driven Biothreats: Emerging Risks and Countermeasures*, 2025. https://www.researchgate.net/publication/389148605_AI-Driven_Biothreats_Emerging_Risks_and_Countermeasures.
- Dixon, Thom, «The grey zone of cyber-biological security», *International Affairs*, vol. 97, fasc. 3, maggio 2021, pp. 685–702.
- Elgabry, Mariam, Shane Johnson, «Cyber-biological convergence: a systematic review and future outlook», *Frontiers in Bioengineering and Biotechnology*, vol. 12, fasc. 1456354, 2024. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11458441/>.
- George, Asha M., «The National Security Implications of Cyberbiosecurity», *Frontiers in Bioengineering and Biotechnology*, vol. 7, marzo 2019. <https://www.frontiersin.org/journals/bioengineering-and-biotechnology/articles/10.3389/fbioe.2019.00051/full>.
- Gomez, Dr Rafael J., «Cyberbiosecurity: The New Frontier of Protection», *Journal of Bioterrorism & Biodefense*, vol. 16, fasc. 6, 2025, pp. 1–4.
- Kastelic, Andraz, Louison Mazeaud, «Cyberbiosecurity: A Matter of International Peace and Security?», 2025. <https://unidir.org/publication/cyberbiosecurity-a-matter-of-international-peace-and-security/>.
- de Lima, Renan Chaves, Juarez Antonio Simões Quaresma, «Emerging technologies transforming the future of global biosecurity», *Frontiers in Digital Health*, vol. 7, giugno 2025. <https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2025.1622123/full>.
- National Academies of Sciences, «Promoting and Protecting AI-Enabled Innovation for Biosecurity», *The Age of AI in the Life Sciences: Benefits and Biosecurity Considerations*, National Academies Press (US), 2025. <https://www.ncbi.nlm.nih.gov/books/NBK614605/>.
- National Academies of Sciences, Engineering, and Medicine, «Biotechnology in the Age of Synthetic Biology», *Biodefense in the Age of Synthetic Biology*, 15–22, Washington D.C., The National Academic Press, 2018. <https://www.nationalacademies.org/read/24890/chapter/1>.
- Okon, Michael Ben, Okechukwu Paul-Chima Ugwu, Chinyere Nneoma Ugwu, Fabian Chukwudi Ogenyi, Dominic Terkimbi Swase, Chinyere Nkemjika Anyanwu, Val Hyginus Udoka Eze, et al., «From pandemics to preparedness: harnessing AI, CRISPR, and synthetic biology to counter biosecurity threats», *Frontiers in Public Health*, vol. 13, novembre 2025. <https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1711344/full>.

Wang, Mengdi, Zaixi Zhang, Amrit Singh Bedi, Alvaro Velasquez, Stephanie Guerra, Sheng Lin-Gibson, Le Cong, et al., «A call for built-in biosecurity safeguards for generative AI tools», *Nature Biotechnology*, vol. 43, fasc. 6, giugno 2025, pp. 845–847.

Zhang, Zaixi, Souradip Chakraborty, Amrit Singh Bedi, Emilin Mathew, Varsha Saravanan, Le Cong, Alvaro Velasquez, et al., «Generative AI for Biosciences: Emerging Threats and Roadmap to Biosecurity», arXiv, novembre 4, 2025. <http://arxiv.org/abs/2510.15975>.

«Cyberbiosecurity and Espionage», *Cyberbiosecurity*, 2022. https://www.cyberbiosecurity.ch/Espionage_Cyberbiosecurity.html.



SpecialEurasia
Geopolitical Intelligence & Risk Assessment

ONLINE COURSE IN OPEN SOURCE INTELLIGENCE

SATURDAY, 23 MAY 2026 | 0900 - 1300 CET

www.specialeurasia.com

info@specialeurasia.com



SpecialEurasia

Online Course in Geopolitical Intelligence Analysis

Saturday, 6 June 2026 | 0900 - 13000 CET

www.specialeurasia.com
info@specialeurasia.com



SpecialEurasia

Website: www.specialeurasia.com

E-mail: info@specialeurasia.com

Copyright © 2026 SpecialEurasia

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial use permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permission Coordinator,” at info@specialeurasia.com.