Preprints.org

Review

Not peer-reviewed version

Mirror Biology and Cyberbiosecurity: New Frontiers, Risks, and Strategic Responses

Sebunya Emmanuel Kato *, Erikan Baluku, Rosemond Nyatefe Tawiah, Charity Serwaa, Simon Anguzu, Hazvinei Mang'anda, Lucas Potter *, Abigarl Ndudzo, Joseph Twizerimana, Xavier Palmer, Kisuule Shamirah

Posted Date: 29 October 2026

Keywords: mirror biology; cyberbiosecurity; synthetic organisms; adversarial bioinformatics; governance; risk assessment

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC, OpenAlex.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Review

Mirror Biology and Cyberbiosecurity: New Frontiers, Risks, and Strategic Responses

Sebunya Emmanuel Kato [1,*], Erikan Baluku [2], Rosemond Nyatefe Tawiah [3], Charity Serwaa [4], Simon Anguzu [5], Hazvinei Mang'anda [6], Lucas Potter [7,*], Abigarl Ndudzo [8], Joseph Twizerimana [9], Xavier Palmer [7] and Kisuule Shamirah [5]

[1] SynBio4ALL Africa, France
[2] SynBio4ALL Africa, New Zealand
[3] SynBio4ALL Africa, Canada
[4] SynBio4ALL Africa, Ghana
[5] SynBio4ALL Africa, Uganda
[6] SynBio4ALL Africa, Malawi
[7] BIOSView, USA
[8] SynBio4ALL Africa, Kenya
[9] SynBio4ALL Africa, Rwanda
* Correspondence: emmasebunyakato@synbioforall.org (S.E.K.); biosview1@proton.me (L.P.)

Abstract

Mirror biology is the creation of synthetic organisms composed entirely of mirror-image biomolecules, such as D-amino acids and L-sugars, in contrast to the natural use of L-amino acids and D-sugars. Though this novel field promises significant advances in medicine, biomanufacturing, and environmental applications due to the enhanced stability and immune evasion of mirror organisms, its features raise unprecedented biosecurity risks, particularly when combined with cybersecurity vulnerabilities in the digital infrastructures used to design, synthesise, and control mirror life. We mapped the mirror biology development pipeline, from genetic circuit design and cloud-based bioinformatics to automated laboratory systems, to examine the unprecedented biosecurity risks associated with mirror biology. We highlighted key cyber biosecurity vulnerabilities, including data manipulation, unauthorised access, and firmware tampering. Case studies illustrate specific risks such as tampering with genetic design tools and introducing harmful DNA sequences into supply chains. The paper reviews existing technological safeguards, including encryption, zero-trust architectures, AI-enabled anomaly detection, and governance mechanisms such as biosafety oversight and redline enforcement. It emphasises the need for inclusive governance, capacity building, and international collaboration to ensure that mirror biology is not pursued as a field of organism- level research.

Keywords: mirror biology; cyberbiosecurity; synthetic organisms; adversarial bioinformatics; governance; risk assessment

1. Introduction

Within synthetic biology, mirror biology has emerged as a highly distinctive and potentially high-consequence frontier. This field emphasises the design and synthesis of mirror-image biomolecules and, ultimately, mirror organisms in contrast to conventional biological systems that rely on natural chirality. This paradigm shift offers substantial scientific opportunities while simultaneously introducing novel biosecurity and governance challenges that existing frameworks are inadequately prepared to address. This paper focuses specifically on organism-level mirror biology and its intersection with cyberbiosecurity. Rather than reiterating general cyberbiosecurity risks throughout, we use the introduction to establish why mirror organisms represent a qualitatively

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

different category of synthetic biological systems and why their emergence requires an integrated cyber–biological security perspective.

The remainder of the paper proceeds in four structured steps. First, we summarise current scientific understanding of mirror biology and outline the unique biosecurity questions it raises. Second, we introduce core cyberbiosecurity concepts only as needed to understand how digital infrastructures enable, mediate, or constrain mirror-life development. Third, we develop scenario-based analyses that link cyber intrusions to plausible mirror-biology outcomes, highlighting where existing risk models may fall short. Finally, we propose a mirror-biology-specific cyberbiosecurity framework that maps pipeline stages, assets, threats, and controls, and we situate its governance implications within broader international policy debates.

This structure is intentionally designed to move from foundational concepts toward a concrete, mirror-life–specific analytical framework. By doing so, the paper avoids redundancy, strengthens conceptual clarity, and makes its contributions to counterproliferation and governance explicit from the outset.

In recent decades, advancements in biotechnology have revolutionised fields ranging from healthcare to agriculture to environmental conservation. Simultaneously, cybersecurity has emerged as a critical discipline for protecting digital systems integral to modern life. The convergence of biotechnology and cybersecurity, termed "cyberbiosecurity," has rapidly become a critical area of research due to the expanding digital and physical interface between computational systems and biological entities (Murch et al. 2018; Greenbaum, Field, and Threats, n.d.). Within this context, mirror biology represents a particularly fascinating and consequential new frontier. Mirror biology involves creating biological organisms or biomolecules that are exact mirror images (enantiomers) of naturally occurring life forms, relying entirely on molecules with opposite chirality (Pedroni et al. 2025). While naturally occurring life predominantly uses left-handed (L-) amino acids and right-handed (D-) sugars, mirror biology attempts to construct organisms using right-handed (D-) amino acids and left-handed (L-) sugars (Adamala, Agashe, Belkaid, et al. 2024). Such organisms, called mirror organisms, promise remarkable applications in medicine, biotechnology, and synthetic biology due to their inherent resistance to enzymatic degradation and immune system evasion (Adamala, Agashe, Binder, et al. 2024).

However, this unique resistance also represents an unprecedented biosecurity threat. Mirror organisms, particularly mirror bacteria, could potentially circumvent conventional biological control mechanisms, evade immune detection, and disrupt ecological balance (Adamala, Agashe, Belkaid, et al. 2024). Their altered chirality fundamentally changes interactions with natural organisms, making them resistant to standard defense mechanisms such as immune recognition, predation, and biodegradation. Consequently, mirror organisms could proliferate unchecked, posing significant risks to human, animal, and plant health, as well as ecosystems at large (Adamala, Agashe, Binder, et al. 2024). These biosecurity concerns are compounded by significant cybersecurity vulnerabilities inherent in modern biotechnology infrastructure. Laboratories increasingly depend on highly automated, digitally controlled systems for the synthesis, design, and deployment of synthetic organisms (A. J. Titus, K. E. Hamilton 2023). Thus, the synthesis of mirror organisms could become vulnerable to cyber threats ranging from digital espionage and intellectual property theft to deliberate sabotage and terrorism. The sensitive digital interfaces used to engineer and produce mirror life forms provide multiple new avenues for malicious actors to exploit, potentially leading to the misuse or unintended dissemination of mirror organisms (A. J. Titus, K. E. Hamilton 2023).

Given these dual-layered threats, a comprehensive, integrated approach to cyberbiosecurity is crucial. Such an approach integrates robust biological safety protocols with novel cybersecurity measures to protect bioinformatics data, synthetic biology processes, and digital infrastructure from sophisticated cyber threats (Murch et al. 2018; A. J. Titus, K. E. Hamilton 2023). Proactive implementation of cyberbiosecurity measures, interdisciplinary cooperation, and rigorous governance structures are imperative for managing and mitigating the risks posed by the rapidly developing field of mirror biology. This paper explores the complex interplay between mirror biology

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

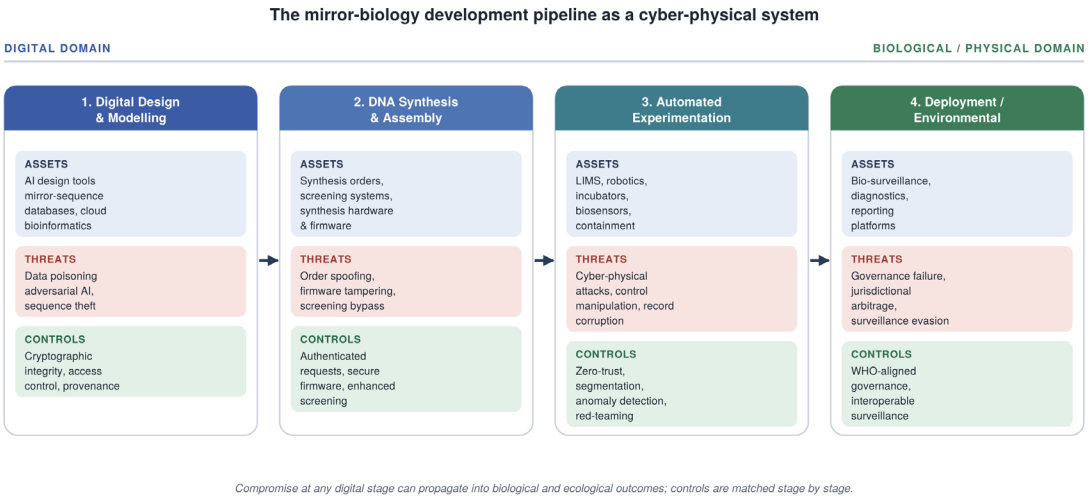
and cyberbiosecurity, providing a detailed examination of their intersections, inherent risks, and proposing strategies and frameworks necessary for risk governance, prevention, and preparedness in this emerging technological landscape. By addressing these converging threats early, the scientific community can strengthen preparedness, reduce the risk of misuse, and improve governance of mirror biology without compromising public health, ecological stability, or global biosecurity.

In this review, we adopt a precautionary, counterproliferation-oriented stance on mirror biology. Drawing on emerging scientific and policy analyses, we consider the deliberate creation of self-replicating mirror organisms to be an unacceptable direction for experimental work under present and foreseeable conditions because the potential for biological threat and irreversible harm far outweighs any future benefits. Our discussion of the mirror-biology 'pipeline' is therefore analytic rather than aspirational: it illustrates how such capabilities could emerge despite opposition and identifies digital and physical leverage points where they can be prevented, detected, or disrupted. Within this framing, the cybersecurity measures we discuss are intended to constrain and deter the realization of mirror life, not to enable its development.

1.1. Contribution and Significance of the Review

This review addresses an emerging gap at the intersection of mirror biology and cyberbiosecurity. Recent work has substantially advanced understanding of the feasibility, potential benefits and biological, ecological and biosafety implications of mirror organisms, culminating in calls for precautionary assessment of self-replicating mirror life (Adamala et al., 2024). More recently, the UK Government Office for Science emphasized the importance of distinguishing research on individual mirror molecules and components from the development of self-replicating mirror organisms, while considering risks across the developmental pathway (Government Office for Science, 2025). However, these discussions have not yet been systematically integrated with the cyberbiosecurity implications of increasingly digital, automated and interconnected biological research.

The principal contribution of this review is to bridge mirror biology and cyberbiosecurity within a common risk framework. Rather than treating mirror-life risks exclusively as biological or ecological hazards, we conceptualize its development as a cyber-physical pipeline extending from digital sequence design, computational modeling and information exchange through DNA synthesis, automated experimentation, characterization, storage and potential deployment (Elgabry & Johnson, 2024; Kato et al., 2026). This approach builds on emerging cyberbiosecurity scholarship showing that the increasing convergence of engineered biology with digital infrastructure, automation, artificial intelligence, biological datasets and supply chains creates vulnerabilities that cannot be adequately addressed through conventional biosafety or cybersecurity measures alone (Liu et al., 2024). (Figure 1).



© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

Figure 1. The mirror-biology development pipeline conceptualized as a cyber-physical system. Each stage couples critical digital and biological assets with stage-specific threats and matched technical and governance controls. A compromise in the digital domain can propagate downstream into biological and physical outcomes.

A second contribution is the development of a mirror-biology-specific cyber-physical vulnerability framework that maps potential digital, cyber and cyber-physical vulnerabilities onto successive stages of the mirror-biology pipeline. This extends existing cyberbiosecurity frameworks, which have identified vulnerabilities associated with biological information, connected laboratory systems, automated biofoundries and supply-chain infrastructure Elgabry & Johnson, 2024), by examining how such vulnerabilities could intersect with the distinctive biological characteristics and potential consequences of mirror organisms (Shankar et al., 2024).

Third, the review advances a scenario-based analysis of cascading risk, linking potential cyber compromise at different points in the development pipeline to downstream biological, ecological, health and socio-economic consequences. This shifts the analytical focus from whether an individual cyber vulnerability exists to how a compromise could propagate across interconnected digital and biological systems (Fouad et al., 2024; Elgabry & Johnson, 2024). Such lifecycle and convergence-based analysis is increasingly recognized as necessary for governing emerging cyberbiosecurity risks.

Finally, the review translates these technical and biological considerations into governance, regulatory and capacity-building priorities. Rather than advocating blanket restrictions on mirror-biology research, it supports risk-proportionate governance that distinguishes lower-risk work on mirror components from research involving self-replicating mirror organisms, while incorporating cybersecurity, information governance, secure-by-design principles, responsible data management and international coordination. This distinction is particularly important for ensuring that governance mechanisms address genuine risks without unnecessarily constraining potentially beneficial applications of mirror chemistry and biology (Government Office for Science, 2025; Kato et al., 2026). Recent work on synthetic-biology governance in Africa similarly identifies resource, expertise and regulatory-capacity gaps, underscoring the importance of internationally inclusive approaches to emerging biotechnology governance (Baluku et al., 2026).

Taken together, the significance of this review lies in providing an integrated analytical bridge between the emerging biological risks of mirror life and the digital vulnerabilities of modern biotechnology. It therefore complements existing assessments of mirror-life safety and ecological risk while extending cyberbiosecurity thinking to a prospective biotechnology whose development could increasingly depend on interconnected computational, automated and biological infrastructures.

2. Fundamentals of Mirror Biology

Mirror biology involves the synthesis of biological systems composed entirely of mirror-image (enantiomeric) molecules that differ in chirality, a property describing non-superimposable mirror images of biomolecules. Recent progress in synthetic chemistry has enabled the creation of mirror-image proteins and nucleic acids. Techniques such as solid-phase peptide synthesis (SPPS) and native chemical ligation enable the production of complex mirror enzymes necessary for replication and transcription of mirror nucleic acids (Adamala, Agashe, Belkaid, et al. 2024). These capabilities support bottom-up approaches, in which mirror components are chemically synthesised and assembled into self-replicating systems within mirror membranes. A theoretical top-down approach that gradually replaces natural biomolecules with mirror equivalents has also been proposed, though it faces significant technical challenges due to incompatibilities between mirror and natural molecules (Adamala, Agashe, Binder, et al. 2024). While mirror biology offers potential for stable, long-lasting therapeutics, it also raises serious biosecurity concerns, as such organisms may evade detection and resist conventional containment or treatment methods. This highlights the need for robust governance, thorough risk assessment, and stringent oversight. (Figure 2).

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

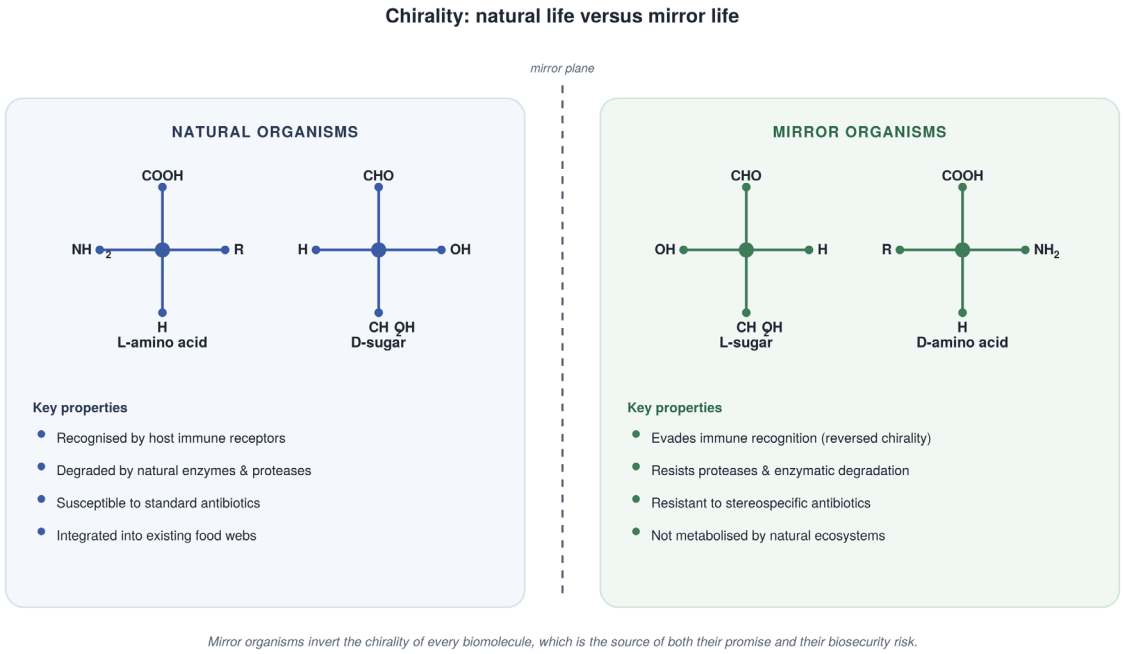


Figure 2. Chirality in natural versus mirror life. Natural organisms are built from L-amino acids and D-sugars, whereas mirror organisms invert the chirality of every biomolecule, using D-amino acids and L-sugars. This reversal underlies both the proposed benefits (stability, immune evasion) and the biosecurity concerns (resistance to enzymatic degradation, antibiotics, and natural biological controls).

3. Cyberbiosecurity: Concept and Importance

Cyberbiosecurity is an emerging field that examines how vulnerabilities in digital infrastructure can translate into biological consequences (Murch et al. 2018; A. J. Titus, K. E. Hamilton 2023). In this section, we briefly introduce some core concepts, including cyberphysical interfaces, data integrity, and automation security, that are needed to better understand later sections. We deliberately limit this overview to ideas that will be used in our mirror-biology case, rather than providing a general survey of cyberbiosecurity. Subsequent sections apply these concepts directly to the mirror biology pipeline. The core aim of cyberbiosecurity is to safeguard the integrity, security, and resilience of the global bioeconomy. This bioeconomy encompasses sectors such as agriculture, pharmaceuticals, healthcare, biotechnology, and synthetic biology (A. J. Titus, K. E. Hamilton 2023). As biotechnology increasingly depends on advanced digital infrastructure, including cloud-based databases, automation systems, artificial intelligence (AI)-driven analytical tools, and bioinformatics software, the potential for cyber vulnerabilities and targeted attacks correspondingly grows. Central to cyberbiosecurity is the recognition of unique vulnerabilities that arise from the integration of digital systems and biological processes. Unlike traditional cybersecurity, cyberbiosecurity specifically addresses scenarios in which cyber-attacks could directly impact biological outcomes, such as the synthesis of organisms or modification of genetic data (Greenbaum, 2023). Examples of potential cyber threats include unauthorized access to genomic databases, manipulation of synthetic biology design tools, sabotage of automated biomanufacturing processes, and cyber intrusions into healthcare and agricultural biosecurity systems. Moreover, cyberbiosecurity emphasizes the potential cascading effects of a cyber incident, ranging from localized disruptions in laboratory activities to large-scale ecological or public health crises. Interestingly, the Safeguarding the Bioeconomy report specifically identified cybersecurity vulnerabilities and data integrity as central risks to the U.S. bioeconomy, directly relevant to the digital infrastructure underpinning mirror biology research. Given the scale and critical importance of bioeconomic activities, even minor security breaches could escalate rapidly, underscoring the need for proactive, integrated security frameworks.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

Implementing cyberbiosecurity practices requires interdisciplinary collaboration across sectors and disciplines, including biology, bioinformatics, cybersecurity, engineering, and policy-making. Such collaboration helps to develop comprehensive strategies capable of addressing multifaceted threats (Murch et al. 2018). Additionally, cyberbiosecurity employs advanced cybersecurity methodologies like zero-trust models, continuous authentication, role-based access control, and AI-driven threat detection systems to secure sensitive biological information and protect against sophisticated cyber-attacks (A. J. Titus, K. E. Hamilton 2023). In the context of rapidly advancing technologies such as mirror biology, cyberbiosecurity becomes even more essential. The inherent biosecurity risks posed by mirror organisms, coupled with cybersecurity vulnerabilities in the digital infrastructures that support their creation, underscore the importance of robust cyberbiosecurity frameworks. Thus, cyberbiosecurity is a central, strategic necessity for reducing risk and strengthening governance of emerging biotechnologies.

4. Risks and Challenges of Mirror Biology

The development and application of mirror organisms, especially mirror bacteria, introduces unprecedented risks and challenges due to their biological distinctness and resistance to traditional biological systems. The health of people, animals, and plants, as well as the stability of the ecosystem as a whole, are all in danger because mirror organisms are resistant to typical immune system responses, they offer one of the biggest biosecurity risks. In humans, animals, and plants, immune recognition mostly depends on stereospecific interactions between microbial antigens and immune receptors. Due to their reversed chirality, mirror organisms are unlikely to be recognized by host pattern recognition receptors (PRRs), potentially compromising innate immune detection. Empirical studies are needed to confirm this hypothesis. Existing antimicrobial treatments, including antibiotics, rely predominantly on stereospecific molecular interactions, potentially rendering most existing therapeutics ineffective against mirror organisms (Kleinman, Torres, and Wang 2026). Although chirality mismatch may prevent mirror bacteria from naturally infecting humans, they could withstand standard therapies intended for natural biomolecular interactions if they are modified to engage with host systems. This resistance to conventional therapies may exacerbate public health situations, making response plans more challenging and increasing rates of morbidity and mortality (Adamala, Agashe, Belkaid, et al. 2024).

Because mirror bacteria are thought to be immune to bacteriophages and natural predators, they pose ecological problems. Since natural biological controls are unable to recognize and effectively eradicate mirror bacteria, they may theoretically proliferate artificially or in controlled environments. However, because of their reversed chirality, mirror organisms may be metabolically incompatible in their natural environment unless they have been engineered to be similar to D-form chirality, which would limit their ecological survival. Furthermore, the adaptability and potential resilience of mirror organisms exacerbate these ecological risks. While initial mirror organisms may be designed with containment strategies in mind, their inherent resistance to degradation and predation could facilitate environmental persistence and spread, especially if containment measures fail or are intentionally circumvented. This scenario raises concerns about potential misuse or accidental release, emphasizing the critical need for rigorous containment protocols and stringent oversight (Adamala, Agashe, Binder, et al. 2024). Lastly, the ethical and regulatory challenges associated with mirror biology are substantial. The profound uncertainty and potentially severe consequences of creating mirror organisms necessitate clear ethical guidelines, comprehensive risk assessments, and robust governance structures. The interdisciplinary nature of these challenges requires collaboration among researchers, policymakers, ethicists, and the broader international community to ensure safe and responsible development in this emerging field.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

5. Cybersecurity Vulnerabilities in Mirror Biology Research and Development

The reliance of mirror biology research on digitised systems, such as computational design platforms, automated laboratory instrumentation, and artificial intelligence tools, poses cybersecurity concerns. This is because digital interconnectivity creates vulnerable opportunities for attack (Shankar et al. 2024; Crawford et al. 2023). Cybersecurity vulnerabilities arise from digital technologies, with biological systems and databases exposed to malicious actors. These vulnerabilities include the possibility that malevolent entities could engineer and duplicate self-replicating biological systems (Elgabry and Johnson 2024). The bio-cyber interface risk is the exposure of sensitive biomechanisms to cyber threats due to unauthorised access and biodata privacy breaches (Zafar et al. 2021). Internet-connected high-containment research labs are particularly vulnerable. A hack could harm public health and compromise the integrity of science (Crawford et al. 2023). Cyberattacks could go after biological databases, such as genomic sequences. Cyberattacks can corrupt such biomedical information, creating a "mirror life" for malicious use and potentially having significant public health implications (Crawford et al. 2023). Cyber-physical attacks pose a distinct risk to mirror biology because they target the control systems that manage automated experiments and containment infrastructure. In a typical automated mirror-biology workflow, programmable pumps, incubators, and biosafety cabinets receive digital control signals from networked computers. An attacker who compromises these control channels could, for example, alter temperature profiles, nutrient flows, or even sterilization cycles in ways that could favor the growth or persistence of mirror organism cultures while leaving logs that appear normal (Mikhaylenko and Zhang 2024). Even if the attacker has only approximate knowledge of the underlying models, standard control-theory techniques can be used to nudge a system toward unsafe states without triggering simple threshold alarms (Mikhaylenko and Zhang 2024). This kind of attack is particularly concerning for mirror biology because the organisms involved are not recognized by standard biosurveillance tools.

In parallel, adversaries may exploit the digital workflows that translate sequence designs into synthesis orders by incorporating malware-like patterns in DNA constructs that interfere with analysis software or by corrupting the configuration of sequence-screening tools (Liu et al. 2024). Finally, the theft and manipulation of any bioinformation could lead to mirror-biology weapons, raising security concerns (Fouad 2024). Other cyber-physical risk pathways identified at the interface of mirror biology and cyberspace include automated bio-foundries, cloud labs, AI-driven design tools, decentralized data sharing, digital biomanufacturing pipelines, and cyber-mediated supply chains (Elgabry and Johnson 2024). Together, these cyber-physical and data-centric attack paths illustrate how compromising digital sequences could directly change biological outcomes.

Studies suggest the following policy recommendations: establishing cross-disciplinary training programs, enhancing biosurveillance with AI tools, improving access control to synthetic biology databases, creating international cybersecurity standards for bio-data, encouraging dual-use awareness, regulating automated bio-design platforms, establishing cyberbiosecurity risk assessment frameworks, mandating red-team audits in synthetic biology facilities, and finally supporting R&D for cyber-resilient bio infrastructure (Elgabry and Johnson 2024). The technical solution includes secure-by-design platforms for mirror biology databases, expanding DNA synthesis screening guardrails to include checks for mirror-coded sequences, and finally, red-team drills to identify weaknesses around mirror biology laboratories (Murch et al. 2018; Liu et al. 2024). Therefore, as mirror biology opens doors to innovative research technologies, there is a need for proactive measures to prevent unauthorized access and misuse, and unintended realization of mirror biology capabilities.

Table 1 summarises attack vectors relevant to mirror biology, their mechanisms, targeted systems, potential outcomes, and illustrative mitigation strategies.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

Table 1. Attack vectors relevant to mirror biology: mechanisms, targeted systems, potential outcomes, and illustrative mitigation strategies.

Potential Attack Vector	Technical Mechanism	Targeted Systems	Potential Outcomes	Mitigation Strategies
1. Bio-database compromise	Unauthorised access; data corruption	Genomic and mirror-sequence repositories	Altered biological designs; data integrity loss	Access controls; integrity verification
2. Cyber-physical laboratory intrusion	Signal manipulation; firmware tampering	Automated lab systems; containment infrastructure	Experimental disruption; containment breach	Network segmentation; real-time monitoring
3. Synthetic DNA exploitation	Malware DNA; malicious code insertion	Gene synthesis pipelines; lab software	Novel bio-threats; workflow compromise	Sequence screening; secure pipelines
4. Supply-chain interference	Order spoofing; logistics manipulation	Reagent suppliers; ordering systems	Unauthorised production; contamination risks	Vendor vetting; provenance tracking
5. AI design manipulation	Data poisoning; adversarial inputs	Machine learning and design tools	Unsafe or unintended biological constructs	Model auditing; dataset validation

6. Integrated Risk Scenario Analysis

The creation of mirror biological systems, particularly mirror bacteria composed of D-amino acids and L-sugars, has prompted increasing discussion regarding their potential risks to human health, ecosystems, and global biosecurity. Mirror biology questions basic assumptions in biochemistry, immunology, and ecology because many biological processes are inherently stereospecific. Although early studies point to significant theoretical dangers, experts still debate how serious these risks are and how likely or imminent they are. Most risks are predictions rather than proven facts, since mirror biology is still new and no fully independent mirror organisms exist yet. (Figure 3).

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

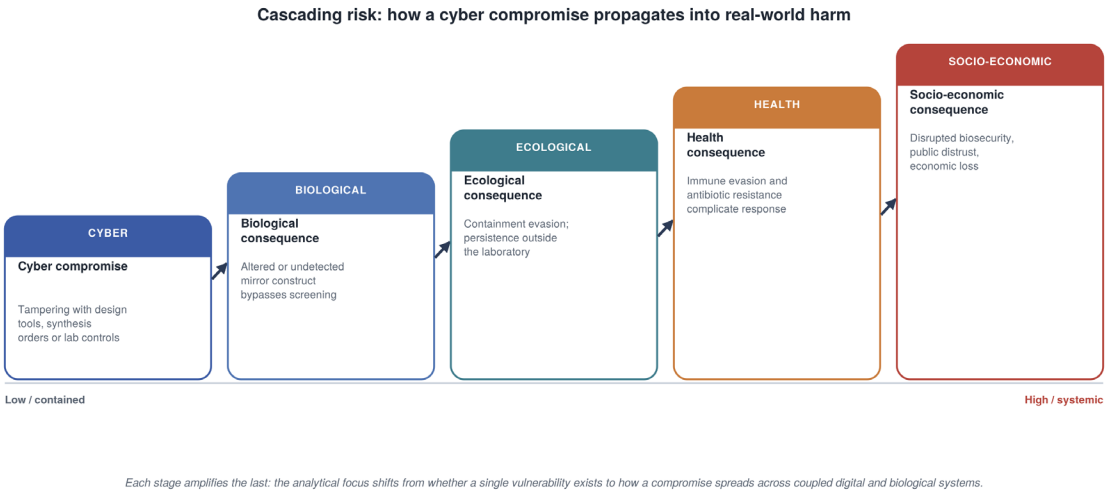


Figure 3. Cascading risk from a cyber compromise to real-world harm. A single intrusion at an early pipeline stage can propagate into biological, ecological, health, and socio-economic consequences, with impact escalating from contained to systemic. The analytical focus therefore shifts from whether an individual vulnerability exists to how a compromise spreads across coupled digital and biological systems.

One of the most frequently cited concerns is that mirror organisms might evade immune detection because their molecular structures do not match the host's pattern recognition receptors (PRRs), antibodies, or antimicrobial peptides. In principle, their reversed chirality could make them hard for the immune system to recognize, similar to how non-natural peptides can resist proteolysis in vitro (Link, Mock, and Tirrell 2003). Since immune systems depend on matching molecular shapes, mirror biomolecules might not attach to immune receptors, making them nearly invisible to the immune system. In the same way, most antibiotics work by interacting stereospecifically with specific bacterial targets, so mirror organisms could be naturally resistant to standard antimicrobial therapies (Adamala, Agashe, Belkaid, et al. 2024; Peplow 2025). However, some experts point out that being invisible to the immune system does not mean an organism can cause disease. Most harmful microbes require molecular compatibility with their host to infect it. So far, mirror organisms have not been shown to infect normal hosts. Some researchers believe mirror bacteria would be isolated by their chemistry rather than by their ability to invade. Causing disease usually requires more than just avoiding the immune system; it also requires the ability to obtain nutrients and enter cells, which mirror organisms do not have unless they are heavily engineered. Currently, there is no published evidence that mirror cells can infect or survive in mammals, plants, or insects.

Mirror organisms would need their own versions of key molecules, like nucleotides and sugars, to survive. Since natural environments mostly contain the usual molecular forms, there is no evidence that mirror organisms can use L-substrates effectively (Schwille 2011). So, even if they could avoid the immune system, it might not matter if they cannot live or grow in hosts. If mirror organisms ever become a demonstrated threat, their chemistry might also inform countermeasures tailored to them. In fact, drug designs based on mirror peptide resistance have already produced stable, protease-resistant compounds, showing that molecular shape is a design choice, not a roadblock (McConathy and Owens 2003). Without empirical infection data, the risks of immune evasion and antibiotic resistance remain theoretical and depend on future advances in engineering. Also, the assumption that mirror organisms could resist treatment assumes they would actually matter in a clinical setting. While mirror enzymes may resist existing antibiotics, mirror organisms would not be able to use the host's nutrients, hormones, or cofactors unless they are supplied with mirror analogues. This need for specialized resources would make it hard for them to survive outside the lab, greatly limiting their real-world risk in the near future.

Some ecological risk assessments suggest that mirror organisms could evade biological control mechanisms, such as predators, parasites, and bacteriophages, thereby growing unchecked. While

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

bacteriophages are indeed very specific to their hosts, the real impact depends on whether mirror organisms can actually compete for resources and replicate outside the lab. In principle, the absence of natural mirror phages or predators could lead to reduced population control (Adamala, Agashe, Binder, et al. 2024). On the other hand, many researchers believe that mirror organisms would be isolated in nature rather than spreading freely. Most natural ecosystems use L-biochemistry, so mirror organisms could not use normal nutrients, break down organic matter, or join microbial communities without mirror versions of these substances. Without a steady supply of D-nutrients, mirror organisms would likely be outcompeted or become inactive (Schwille 2011). This means they would not last in the environment unless special mirror ecosystems are built or heavily supported. Because they do not fit into normal food webs, it is unlikely they would spread on their own. So far, no studies have shown that mirror organisms can survive outside tightly controlled lab settings. Therefore, predictions about environmental risks remain speculative and depend heavily on how these organisms are designed.

From a biosecurity perspective, the main concern about mirror biology is not proven harm but its potential for misuse. Being able to create organisms that resist current biological controls makes it harder for biosurveillance, risk modeling, and biodefense systems to keep up. In cyberbiosecurity, mirror organisms also complicate matters because current databases, detection tools, and genome classifiers assume the usual molecular shapes (Peccoud et al. 2018; Murch et al. 2018). These are real challenges in theory, but they only become serious if mirror organisms are actually created and used. Most experts agree that the main biosecurity risk is not a proven biological threat but a policy and regulatory gap. Current regulatory frameworks and risk assessment models are not designed to handle organisms that deviate from normal biochemistry (National Academies of Sciences, Engineering 2018). This delay in regulation makes it easier for mirror biology to be misused, accidentally released, or misinterpreted in early experiments. Nonetheless, there are no known cases of mirror biology being used as a weapon or outside of lab research.

The ethical debate surrounding mirror biology is marked by significant uncertainty. Some ethicists warn that focusing too much on worst-case scenarios without real evidence could slow down innovation and distract regulators from more pressing risks in synthetic biology (National Academies of Sciences, Engineering 2019). Others support the precautionary principle, calling for oversight that reflects the extent to which these organisms are independent and widely used. It is important to note that there are currently no thorough adversarial risk assessments, such as red-team studies, that quantify probabilities, assess evolutionary limits, and realistic timelines. Supporters of responsible innovation have highlighted this gap. Not having these studies does not mean there is no risk, but it does mean that risk assessments for mirror biology should clearly state what is uncertain and avoid mixing up what is possible in theory with what is likely to happen soon. Several authors call for increased oversight as organisms become more independent and capable, rather than focusing on what might be possible in the distant future (Adamala, Agashe, Belkaid, et al. 2024).

Although mirror biology introduces new risks, most scientists agree that these risks are mostly theoretical, depend on specific conditions, and are unlikely to occur soon. There is general agreement that mirror biology warrants precautionary governance, but debate continues over how dangerous it is in the short term compared to other synthetic biology technologies. The field would benefit from empirical studies on immune responses, metabolic isolation, evolutionary stability, and survival in the environment, as well as from formal red-team analyses to test prevailing assumptions. While immune evasion and antibiotic resistance could happen in highly engineered cases, the lack of metabolic compatibility and host entry points makes spontaneous disease unlikely. The need for specific resources also limits ecological spread. Right now, the biggest risks are gaps in governance, cyberbiosecurity issues, and oversight systems that are not designed for non-standard life forms. To address these gaps, targeted research is needed on how mirror organisms survive, interact with hosts, and can be detected, along with adaptable governance mechanisms that can evaluate novel biology without blocking beneficial innovation. The emerging field would also benefit from structured

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

methods for measuring risk, cross-disciplinary ethical analysis, and international cooperation in oversight.

7. Cyberbiosecurity Frameworks for Mirror Biology

Unlike existing cyberbiosecurity frameworks that primarily address conventional synthetic biology, we propose a mirror-biology-specific cyberbiosecurity framework that systematically links each stage of the mirror biology development pipeline with its associated digital and biological assets, potential threat vectors, technical safeguards and governance mechanisms (Table 2). Rather than presenting cybersecurity recommendations as generic best practices, this framework identifies where cyber compromise could translate into biological consequences unique to mirror biology. It is intended as a counterproliferation tool to identify opportunities to prevent, detect or disrupt the development of organism-level mirror life rather than facilitate its creation.

The framework is organised into four sequential stages: digital design and modelling, DNA synthesis and assembly, automated experimentation and deployment and environmental interface. At each stage, different cyber-physical assets become vulnerable to distinct threats requiring tailored mitigation strategies.

During the digital design and modelling stage, critical assets include computational sequence design platforms, mirror-specific molecular libraries, cloud-based bioinformatics repositories and artificial intelligence models used to optimise biological designs. Since mirror biology begins as digital information before any biological material is produced, cyberattacks at this stage could influence downstream biological outcomes. Potential threats include data poisoning of machine-learning datasets, unauthorised modification of design files, theft of mirror-sequence libraries and adversarial manipulation of AI-assisted design systems. Suitable safeguards include verifying cryptographic integrity, applying role-based access controls, requiring continuous authentication, relying on secure cloud setups, tracking the provenance of design files and subjecting any high-risk mirror-related computational outputs to independent review before they move to laboratory synthesis (Murch et al., 2018; Peccoud et al., 2018). The DNA synthesis and assembly stage introduces additional risks associated with sequence ordering, synthesis hardware, screening software, and laboratory information systems. Existing sequence-screening procedures have already done a great deal to strengthen biosecurity. Still, mirror-related constructs that appear in the future may require extra screening criteria, since most of today's systems were built mainly around canonical biological sequences. Potential threats encompass order spoofing, tampering with the firmware of synthesis instruments, interference with sequence-screening software and unauthorised changes to synthesis requests.

To manage these risks, the recommended steps include requiring authenticated synthesis requests, keeping cryptographically verifiable audit trails, using firmware built with security as a core design principle, carrying out independent sequence verification, and expanding existing sequence -screening protocols so they can also evaluate mirror -related analogues of high-concern biological sequences whenever such assessment is scientifically justified (International Gene Synthesis Consortium; National Academies of Sciences Engineering and Medicine 2020) During automated experimentation, cyberbiosecurity extends beyond data protection into cyber-physical laboratory systems. Critical assets include laboratory information management systems (LIMS), robotic liquid-handling platforms, programmable incubators, sensor networks, automated containment systems and digital twins used to monitor experimental processes. Cyber compromise at this stage could alter environmental parameters, manipulate laboratory records or interfere with containment procedures, thereby producing biological consequences despite apparently normal system operation. Consequently, laboratories conducting high-consequence synthetic biology should implement network segmentation, zero-trust security architectures, continuous monitoring of cyber-physical systems, firmware integrity verification, multi-factor authentication, anomaly detection and regular red-team exercises designed specifically to evaluate cyber-physical laboratory resilience (Murch et al., 2018; National Academies of Sciences Engineering and Medicine 2020).

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

The concluding stage involves deployment or the point at which mirror organisms would interface with the environment. While this review endorses the precautionary perspective that organism-level mirror life ought not to be intentionally released, robust governance frameworks will still be required if mirror-related capabilities arise despite current restrictions. Essential components of such frameworks include environmental surveillance systems, diagnostic laboratories, bio-surveillance databases and international reporting channels.

At this stage, the principal threats are institutional rather than technical, including fragmented governance, inconsistent international oversight, jurisdictional arbitrage and limitations in existing bio-surveillance systems that assume canonical biological chemistry. Mitigation therefore depends upon harmonised international reporting standards, adaptive regulatory oversight, coordinated surveillance networks, transparent information sharing and strengthened international cooperation consistent with the WHO Global Guidance Framework and recent recommendations from the National Academies, NSABB and international reporting mechanisms as emphasised by the World Health Organisation (2022), the National Academies of Sciences, Engineering and Medicine (2018), the National Science Advisory Board for Biosecurity (2023), and the National Security Commission on Emerging Biotechnology (2025)

The framework shows that cyberbiosecurity measures for mirror biology cannot rest solely on standard cybersecurity approaches. Cybersecurity controls must be deliberately matched to the stages of the biological development pipeline and combined with governance systems that can address emerging mirror-biology risks. By connecting each pipeline stage to the relevant assets, threats, technical safeguards and governance responses, the framework offers a workable tool that researchers, laboratory managers, regulators, and policymakers can use to improve preparedness while upholding a precautionary perspective toward organism-level mirror biology.

Table 2. Mirror biology cyberbiosecurity framework: pipeline stages, critical assets, threats, controls, and governance measures.

Pipeline Stage	Critical Assets	Mirror-Specific Threats	Technical Controls	Governance Measures
Digital Design and Modelling	AI-assisted design tools, mirror-sequence databases, molecular libraries, cloud bioinformatics platforms	Data poisoning, adversarial AI inputs, sequence theft, unauthorized modification of design files	Cryptographic integrity verification, role-based access control, provenance tracking, encryption, independent review	Institutional oversight, controlled access to mirror-related computational resources
DNA Synthesis and Assembly	DNA synthesis orders, sequence-screening systems, synthesis hardware, firmware	Order spoofing, firmware tampering, screening bypass, unauthorized sequence modification	Authenticated synthesis requests, secure firmware, cryptographically verifiable audit trails, independent	Compliance with synthesis screening standards (e.g., IGSC), regulatory oversight of

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

			sequence verification, enhanced sequence screening	high-risk synthesis
Automated Experimentation	Laboratory Information Management Systems (LIMS), robotic platforms, incubators, biosensors, containment systems	Cyber-physical attacks, manipulation of environmental controls, protocol alteration, laboratory record corruption	Zero-trust architecture, network segmentation, multi-factor authentication, anomaly detection, firmware integrity monitoring, red-team exercises	Laboratory certification, cybersecurity audits, biosafety and biosecurity compliance
Deployment/Environmental Interface	Bio-surveillance systems, environmental monitoring, diagnostic laboratories, reporting platforms	Governance failure, jurisdictional arbitrage, delayed incident reporting, surveillance evasion	Secure reporting systems, continuous monitoring, interoperable surveillance platforms	WHO-aligned governance, tiered oversight, international reporting, adaptive regulation, cross-border cooperation

Developed by the authors based on concepts synthesized from Murch et al. (2018); Peccoud et al. (2018); National Academies of Sciences, Engineering, and Medicine (2018, 2020); World Health Organization (2022); National Science Advisory Board for Biosecurity (2023); and National Security Commission on Emerging Biotechnology (2025).

8. Policy, Regulation, and Governance

The emergence of mirror-image organisms calls for governance systems that are both rigorous and forward-looking, capable of keeping pace with fast-changing scientific capabilities. Current biotechnology and cybersecurity regulations lack the specificity needed to manage the unique risks associated with mirror-image organisms and the digital design pipelines that support them. Federal Register notices, for example, have already pointed to ambiguities, gaps, inefficiencies, and uncertainties within the coordinated framework for the regulation of biotechnology (K. Molla, Moronta-Barrios, F., Novak, B., Pannu, J., Parthemore, C., Perez, R., Perez-Mercader, J., Ramirez, O., Rath, S., Relman, D. A., Ross, P., Rudenko, L., Sajjad, W., Shamoo, Y., Smith, J., Snyder-Beattie, A., Speight, R., Sundaram, S.,Sung, B. H., 2025). In 2023, the National Science Advisory Board for Biosecurity (NSABB) recommended an integrated approach to oversight that would expand the scope of DURC review, directly addressing the governance landscape that mirror biology would likely fall into (Nih 2023) .

These gaps stem from how tightly biotechnology and digital systems have become intertwined, a point recent analyses have driven home (Murch et al., 2018). The governance steps outlined here take a deliberately cautious perspective. Putting them into practice will mean getting agencies that

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

already share overlapping mandates- public health, research funding, law enforcement and defence to work together more effectively. Even for more familiar biotechnology risks, that kind of coordination has proven difficult. Earlier attempts to align agencies around Dual Use Research of Concern showed both the usefulness of common guidance and how hard it is to apply it consistently across the board. (National Academies of Sciences Engineering and Medicine 2018).

Research by international organisations, including the World Health Organisation, the Organisation for Economic Co-operation and Development, and the Biological Weapons Convention Implementation Support Unit, have provided broad guidance for addressing risks associated with emerging biotechnologies. However, countries have not adopted detailed regulatory standards at the same pace, resulting in differences in how these technologies are governed across jurisdictions (National Academies of Sciences and Medicine,2017). Therefore, measures like tiered oversight, requiring a supermajority for environmental releases, and using blockchain to audit supply chains need to fit the regulatory frameworks and institutional strengths that already exist in each place. They tend to work better when shaped around a country's legal, technical, and governance realities rather than rolled out as a rigid, one-size-fits-all model. Tiered oversight for mirror biology can build on current risk-group and containment frameworks by adding explicit triggers tied to the independence and scalability of mirror systems, for example, moving from local committee review to national-level approval once experiments approach self-replicating mirror cells. Supermajority voting is likely to be the most suitable approach for decisions that could have serious international consequences, especially in established settings such as treaty review conferences and specialised biosecurity committees. These forums already have established procedures for collective decision-making and ready access to scientific advice. Similarly, blockchain-based audit trails could strengthen existing systems for record-keeping and chain-of-custody tracking within gene synthesis and equipment supply chains. Used in this manner, blockchain would function as a supporting technology rather than a replacement for current governance arrangements (Guise et al., 2024).

To reflect the different levels of risk associated with different activities, we suggest a tiered regulatory framework. Level 1 would apply to basic research and would require registration, suitable safety procedures, and regular oversight. Level 2 would cover the synthesis of organisms judged to present higher risks and would call for additional regulatory approval, appropriate containment, and fully traceable records of synthesis activities. Level 3 would address environmental applications and would demand a higher degree of scrutiny, including supermajority approval, formal risk assessment, and ongoing post-release monitoring. The precise containment measures and technical safeguards applied at each level should be decided according to the specific characteristics and assessed risks of the proposed activity (A. Hodgson, Frow, E., Palmer, X.-L., Rohwer, F., Elcock, L., Johnson, A., Zimmerman, E. H., & Voigt 2025). This kind of standardisation helps stop "jurisdictional arbitrage," while still building on the OECD's earlier work in harmonising biotechnology rules (National Academies of Sciences, Engineering, and Medicine, 2017). Proper oversight requires ongoing risk assessment that covers ecological, cybersecurity, and dual-use issues, and these assessments should be done by independent, certified teams. Accountability can be upheld through a system of graduated sanctions, supported by regular audits, mandatory registry reporting, and independent peer review (Weber & Parthermore, 2025). Governance bodies themselves need to bring together a broad mix of stakeholders. For routine licensing decisions, qualified majority voting is usually sufficient, but high-risk applications should require a clear supermajority. Equally important is creating real room for open, cross-sector communication and collaboration if these risks are to be managed effectively (Murch et al.,2018).At the international level, the WHO's 2022 Global Guidance Framework remains the first broad regulatory document aimed at governing dual-use research and mitigating bio risks across member states (World Health Organisation, 2022). Creating "cross-sector convergence opportunities for effective communication and collaboration" proves essential for managing biotechnological risks (Murch et al. 2018). In addition, the National Security Commission on Emerging Biotechnology (NSCEB) in 2025 gave a final report that characterized the current U.S. biosecurity governance as blunt and reactive and recommends a consolidated proactive governance

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

entity specifically capable of addressing AI- enabled sequence design threats (National Security Commission on Emerging Biotechnology (NSCEB) 2025).By rooting these recommendations in the governance practices already in use and recognising the real political and resource limits that shape them, we hope to offer a practical roadmap that policymakers and practitioners can adjust step by step as mirror biology develops, rather than an idealised blueprint that stays out of reach. Research suggest the following policy recommendation: establishing cross-disciplinary training programmes, enhancing biosurveillance with AI tools, improving access control to synthetic biology databases, creating international cybersecurity standards for bio-data, encouraging dual-use awareness, regulating automated bio-design platforms, establishing cyberbiosecurity risk assessment frameworks, mandating red-team audits in synthetic biology facilities, and finally supporting R&D for cyber-resilient bio infrastructure (Elgabry and Johnson 2024). The technical solution includes secure-by-design platforms for mirror biology databases, expanding DNA synthesis screening guardrails to include checks for mirror-coded sequences, and, finally, red-team drills to identify weaknesses in mirror biology laboratories. (Murch et al. 2018; Liu et al. 2024). Therefore, as mirror biology opens doors to innovative research technologies, proactive measures are needed to prevent unauthorised access and misuse of innovations involving mirror biology. (Figure 4).

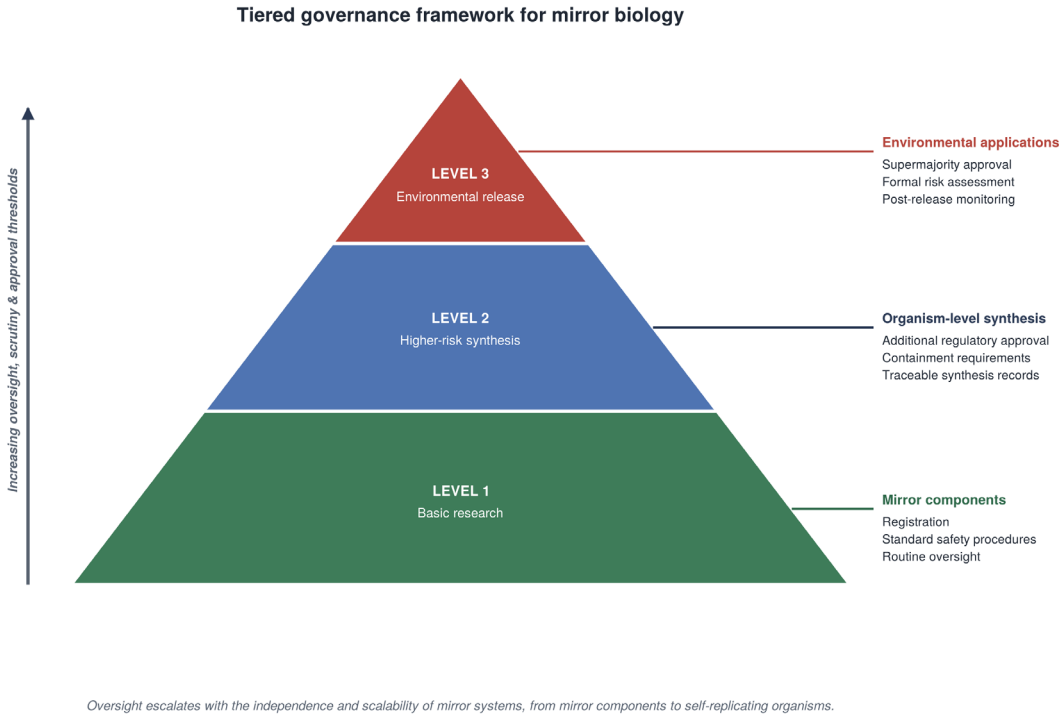


Figure 4. Proposed tiered governance framework for mirror biology. Oversight escalates with the independence and scalability of mirror systems: Level 1 covers basic research on mirror components (registration and routine oversight); Level 2 covers higher-risk, organism-level synthesis (additional approval, containment, traceable records); and Level 3 covers environmental applications (supermajority approval, formal risk assessment, and post-release monitoring).

8.1. Synthesis and Novel Governance Position

The distinctive contribution of this review is the integration of anticipatory mirror-life governance with cyberbiosecurity across the digital-to-biological development lifecycle and not just the proposal of additional biological containment per se. The governance challenge posed by mirror biology is not simply a question of applying existing biosafety rules to a new class of organisms. Rather, it arises from the convergence of synthetic biology, advanced molecular engineering, digital biotechnology and cyberbiosecurity, through which biological systems can increasingly be designed,

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

modeled, ordered and constructed through interconnected digital and physical infrastructures. Recent analyses have highlighted the need to consider biological risks alongside vulnerabilities in data, computational systems, laboratory automation and biotechnology supply chains (Elgabry & Johnson, 2024; Fouad, 2024). For mirror biology, this convergence is significant because the most consequential risks would arise not from individual mirror molecules, but from progression towards self-replicating mirror organisms capable of persistence, spread and ecological interaction.

The emerging scientific consensus supports a precautionary and anticipatory approach. Adamala et al. (2024) argued that the potential consequences of creating self-replicating mirror organisms could be sufficiently severe to justify substantial societal deliberation before such organisms are constructed. The United Nations Secretary-General's Scientific Advisory Board has subsequently called for proactive multilateral action, including clear governance "red lines," strengthened monitoring and international coordination before mirror life becomes technically feasible (United Nations Secretary-General's Scientific Advisory Board, 2026). Importantly, this does not imply that all mirror-biology research should be restricted. Mirror-image proteins, nucleic acids and other non-replicating components may have legitimate applications in medicine, biotechnology and materials science. Governance should therefore distinguish beneficial, non-replicating mirror components from research that materially advances the construction of self-replicating mirror organisms (UK Government Office for Science, 2025).

Building on these developments, this review proposes a Mirror-Biology Cyber-Physical Risk and Governance Framework (MBCRGF). Its principal novelty is the integration of biological risk assessment with cyberbiosecurity across the digital-to-biological development lifecycle. Rather than regulating only the final biological product, governance should encompass the information, computational models, design platforms, DNA/RNA synthesis services, laboratory automation, physical materials, data infrastructures and supply chains that collectively enable biological construction. This approach extends conventional biosafety from containment of biological materials towards cyber-physical governance of the entire development pathway (Elgabry & Johnson, 2024; Fouad, 2024). The framework should operate through risk-based tiers and evidence gates rather than a single blanket regulatory category.

9. Strategic Recommendations for Future Preparedness

To address the dual biosecurity and cybersecurity risks associated with mirror biology, interdisciplinary collaboration should be strengthened through sustained platforms such as workshops, research consortia, and joint funding initiatives that bring together synthetic biologists, cyberbiosecurity experts, bioinformaticians, biosafety and biosecurity specialists, and policy analysts. Cross-disciplinary training and integrated risk-assessment projects can facilitate knowledge exchange and develop the expertise required to identify, assess, and mitigate risks arising at the interface of biological and digital systems (Jannah et al., 2025). The collaboration through cross-training programs and integrated research projects will cultivate the shared expertise necessary for holistic risk management (Jannah, R., Anjum, B. E., Lardner, C., Chappell, C., Palmer, X.-L., Perez, R., Mitra, A., Camenares, D., Seah, A., Kong, D., Elcock, L., Thaweechuen, J., & Flores 2025). Second, international standards and best practices should be established by convening an expert panel to draft global guidelines for mirror-biology cyberbiosecurity. These guidelines must address secure laboratory architectures, encrypted genetic databases, continuous monitoring systems, and rapid containment protocols. Building on existing frameworks like NIST's biosecurity standards for synthetic nucleic acid sequences and the International Gene Synthesis Consortium (IGSC) provides the best practices for DNA screening. The screening standards must be embedded in national biosafety laws to preempt hazardous research trajectories (Relman 2025).

Third, capacity-building and training initiatives are essential for strengthening preparedness among both laboratory scientists and IT professionals. Accredited training programmes should address the biosafety and biosecurity considerations associated with mirror-image organisms, secure handling of biological data, cybersecurity practices, and incident-response procedures. Scenario-

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

based exercises, including controlled laboratory safety simulations and tabletop exercises, could further strengthen workforce readiness and improve coordination during potential biosecurity or cyberbiosecurity incidents (Jannah, R., Anjum, B. E., Lardner, C., Chappell, C., Palmer, X.-L., Perez, R., Mitra, A., Camenares, D., Seah, A., Kong, D., Elcock, L., Thaweechuen, J., & Flores 2025) .

Fourth, governance must be proactive and adaptive rather than reactive. Policies should undergo institutionalized biennial reviews to ensure that regulatory frameworks remain responsive to advances in mirror-organism engineering and AI-driven design tools (Relman 2025). Fifth, public-private and international partnerships should be strengthened to facilitate the sharing of relevant threat intelligence concerning the potential misuse of mirror biology. Coordinated data-sharing mechanisms and joint response exercises involving public agencies, industry R&D laboratories, and nonprofit organizations could strengthen collective preparedness and enable timely detection, assessment, and response to emerging threats (A. Weber, C. Parthemore 2025). Finally, sustained investment in cyberbiosecurity research is required to strengthen preparedness for potential mirror-organism hazards. Dedicated funding should support research on secure bioinformatics platforms, AI-driven threat detection, resilient laboratory-automation systems, and next-generation biocontainment technologies tailored to the distinctive risks associated with mirror biology (Adamala, Agashe, Belkaid, et al. 2024).

10. Conclusions

Mirror biology has emerged as a highly distinctive and potentially high consequences frontier in contrast to the conventional biological systems that rely on natural chirality, it explores the design and construction of mirror-image biomolecules and ultimately mirror organisms. The biggest concern is the deliberate creation of self-replicating mirror organisms whose behaviour in natural systems is uncertain. Moreover, most risks are predictions rather than proven evidence to confirm several of the predicted biological and ecological risks. Future research could depend on synthesis of organisms, genomic databases, manipulation of synthetic biology design tools, sabotage of automated biomanufacturing processes and cyber intrusions into healthcare and agricultural biosecurity systems, creating cyber vulnerabilities. Finally, effective collaboration through cross-training programs and integrated research projects will cultivate the shared expertise necessary for holistic risk management. International standards as well as best practices should be established by convening an expert panel to draft global guidelines for mirror biology cyberbiosecurity.

Author Contributions: S.E.K compiled the final draft with writing and editing inputs from E.B, R.N.T, C.S, S.A, H.M, A.N, J.T, K.S L.P, and X.P. All authors have read and agreed to the submitted version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: All the authors are acknowledged for their equal input in writing this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Informed Consent Statement: Not applicable.

Institutional Review Board Statement: This research did not involve human subjects, personally identifiable data, cell lines, or animal testing. IRB review was not required.

Abbreviations

AI	Artificial intelligence
DURC	Dual Use Research of Concern
IGSC	International Gene Synthesis Consortium

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

LIMS	Laboratory Information Management System
MBCRGF	Mirror-Biology Cyber-Physical Risk and Governance Framework
NIST	National Institute of Standards and Technology
NSABB	National Science Advisory Board for Biosecurity
NSCEB	National Security Commission on Emerging Biotechnology
OECD	Organisation for Economic Co-operation and Development
PRR	Pattern recognition receptor
SPPS	Solid-phase peptide synthesis
WHO	World Health Organization

References

A. Hodgson, Frow, E., Palmer, X.-L., Rohwer, F., Elcock, L., Johnson, A., Zimmerman, E. H., & Voigt, C. 2025. "Public Infrastructure for Analyzing and Assessing Beyond Biocontainment Biotechnologies." Rice University., Presented at the The Spirit of Asimolar and the Future of Biotechnology.

A. J. Titus, K. E. Hamilton, and M. Holko. 2023. "'Cyber and Information Security in the Bioeconomy,' in Cyberbiosecurity: A New Field to Deal with Emerging Threats." Springer, 17–36.

A. Weber, C. Parthemore, and J. Wentzel. 2025. "2.1 Condemning & Making Obsolete Biological Weapons."

Adamala, Katarzyna P, Deepa Agashe, Yasmine Belkaid, Daniela Matias de C Bittencourt, Yizhi Cai, Matthew W Chang, Irene A Chen, et al. 2024. "Confronting Risks of Mirror Life." Science (New York, N.Y.) 386 (6728): 1351–53. https://doi.org/10.1126/science.ads9158.

Adamala, Katarzyna P, Deepa Agashe, Damon J Binder, Yizhi Cai, Vaughn Cooper, Ryan Duncombe, and Kevin Esvelt. 2024. "Technical Report on Mirror Bacteria: Feasibility and Risks." Stanford Digital Repository.

Baluku, E., Kato, S. E., Malemia, S., Tawiah, R. N., Serwaa, C., Namuli, S., Anguzu, S., Mang'anda, H., Mweine, P. and Namugamba, B. (2026). Advancing synthetic biology in African academia: institutional barriers, capacity gaps, and the impact of a pilot online training program. Front. Synth. Biol. 4:1813106. https://doi.org/10.3389/fsybi.2026.1813106

Crawford, Elizabeth, Adam Bobrow, Landy Sun, Sridevi Joshi, Viji Vijayan, Stuart Blacksell, Gautham Venugopalan, and Nicole Tensmeyer. 2023. "Cyberbiosecurity in High-Containment Laboratories." Frontiers in Bioengineering and Biotechnology 11: 1240281. https://doi.org/10.3389/fbioe.2023.1240281.

E. National Academies of Sciences and Medicine. 2017. Preparing for Future Products of Biotechnology. Washington (DC). https://doi.org/10.17226/24605.

Elgabry, Mariam, and Shane Johnson. 2024. "Cyber-Biological Convergence: A Systematic Review and Future Outlook." Frontiers in Bioengineering and Biotechnology 12: 1456354. https://doi.org/10.3389/fbioe.2024.1456354.

Farbiash, Dor, and Rami Puzis. 2020. "Cyberbiosecurity: DNA Injection Attack in Synthetic Biology." http://arxiv.org/abs/2011.14224.

Fouad, Noran Shafik. 2024. "Cyberbiosecurity in the New Normal: Cyberbio Risks, Pre-Emptive Security, and the Global Governance of Bioinformation." European Journal of International Security 9 (4): 553–73. https://doi.org/DOI: 10.1017/eis.2024.19.

D. Greenbaum, Cyberbiosecurity: A new field to deal with emerging threats. Springer, 2023

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

Government Office for Science. (2025). Mirror life: Science advice note-what are the main risks and opportunities associated with researching and developing 'mirror life', including along the pathway of development from cell components to self-replicating cells? https://www.gov.uk/government/publications/mirror-life

Guise, Nicholas, David Pattie, Kenneth B. Yeh, Kemper Talley, and Rachel Fennell Fezzie. 2024. "2023 Cyberbiosecurity Summit Underscores Challenges Associated With Cybersecurity and the Rapidly Growing Bioeconomy." Global Security - Health, Science and Policy 9 (1). https://doi.org/10.1080/23779497.2024.2401164.

Jannah, R., Anjum, B. E., Lardner, C., Chappell, C., Palmer, X.-L., Perez, R., Mitra, A., Camenares, D., Seah, A., Kong, D., Elcock, L., Thaweechuen, J., & Flores, W. N. 2025. "6.3 Community Biology: Advancing Responsible Biotech Innovation." Rice University. https://doi.org/10.25611/3QHJ-W351.

Kato, S. E., Ndudzo, A., Bayiga, S. O., Brenda, N., Serwaa, C., Baluku, E., Mang'anda, H., Peter, J. J., Shamirah, K., Perez, M., Tawiah, R. N., Anguzu, S. & Malemia, S. (2026). Strengthening global biosecurity for synthetic nucleic acid technology: from sequence screening to risk based governance in the AI era. Frontiers in Bioengineering and Biotechnology 14.1820001. https://doi.org/10.3389/fbioe.2026.1820001

K. Molla, Moronta-Barrios, F., Novak, B., Pannu, J., Parthemore, C., Perez, R., Perez-Mercader, J., Ramirez, O., Rath, S., Relman, D. A., Ross, P., Rudenko, L., Sajjad, W., Shamoo, Y., Smith, J., Snyder-Beattie, A., Speight, R., Sundaram, S., Sung, B. H., M. 2025. "Risks from Mirror Life (Spirit of Asilomar Entreaty 2025.4.4." In Spirit of Asilomar Summit.

Kleinman, Alexander, Joe Torres, and Brian Wang. 2026. "Evaluation of Antibiotic and Peptide Vaccine Strategies for Mirror Bacterial Infections," March. https://doi.org/10.7554/elife.109134.1.

Link, A James, Marissa L Mock, and David A Tirrell. 2003. "Non-Canonical Amino Acids in Protein Engineering." Current Opinion in Biotechnology 14 (6): 603–9. https://doi.org/10.1016/j.copbio.2003.10.011.

Liu, Tuoyu, Sijie Zhou, Tao Wang, and Yue Teng. 2024. "Cyberbiosecurity: Advancements in DNA-Based Information Security." Biosafety and Health 6 (4): 251–56. https://doi.org/https://doi.org/10.1016/j.bsheal.2024.06.002.

McConathy, Jonathan, and Michael J Owens. 2003. "Stereochemistry in Drug Action." Primary Care Companion to the Journal of Clinical Psychiatry 5 (2): 70–73. https://doi.org/10.4088/pcc.v05n0202.

Mikhaylenko, Dina, and Ping Zhang. 2024. "Robust Mirror Attacks on Cyber-Physical Systems." In 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT), 724–29. https://doi.org/10.1109/CoDIT62066.2024.10708543.

Murch, Randall S., William K. So, Wallace G. Buchholz, Sanjay Raman, and Jean Peccoud. 2018. "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy." Frontiers in Bioengineering and Biotechnology 6 (APR): 1–6. https://doi.org/10.3389/fbioe.2018.00039.

National Academies of Sciences, Engineering, and Medicine. 2018. National Academies of Sciences, Engineering, and Medicine. Washington (DC). https://doi.org/10.17226/24890.

———. 2019. Framework for Addressing Ethical Dimensions of Emerging and Innovative Biomedical Technologies: A Synthesis of Relevant National Academies Reports. Edited by Leah Rand and Neal Dickert. Washington, DC: The National Academies Press. https://doi.org/10.17226/25491.

National Security Commission on Emerging Biotechnology (NSCEB). 2025. "National Security Commission on Emerging Biotechnology Urges Swift Action to Protect U.S. National Security - Biotech." 2025. https://www.biotech.senate.gov/press-releases/nsceb-publishes-final-report/.

Peccoud, Jean, Jenna E Gallegos, Randall Murch, Wallace G Buchholz, and Sanjay Raman. 2018. "Cyberbiosecurity: From Naive Trust to Risk Awareness." Trends in Biotechnology 36 (1): 4–7. https://doi.org/10.1016/j.tibtech.2017.10.012.

Pedroni, Lorenzo, Chiara Dall'Asta, Gianni Galaverna, and Luca Dellafiora. 2025. "Computational Perspectives on Amoxicillin and Staphylococcus Aureus in Mirror Life." Global Challenges 9 (8): 1–5. https://doi.org/10.1002/gch2.202500051.

Peplow, Mark. 2025. "How Should 'mirror Life' Research Be Restricted? Debate Heats Up." Nature. England. https://doi.org/10.1038/d41586-025-02902-2.

Relman, D. A. 2025. "2.2 The Importance of Redlines in the Life Sciences." Rice University. https://doi.org/10.25611/9XTW-WT37.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org | NOT PEER-REVIEWED | Posted: 29 October 2026 https://doi.org/10.20944/preprints202610.3016.v1

Richardson, Lauren C., Nancy D. Connell, Stephen M. Lewis, Eleonore Pauwels, and Randy S. Murch. 2019. "Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape." Frontiers in Bioengineering and Biotechnology 7 (JUN): 1–5. https://doi.org/10.3389/fbioe.2019.00099.

Schwille, Petra. 2011. "Bottom-Up Synthetic Biology: Engineering in a Tinkerer's World." Science 333 (6047): 1252–54. https://doi.org/10.1126/science.1211701.

Shankar, Deepa D, Adresya Suresh Azhakath, Nesma Khalil, Sajeev J. , Mahalakshmi T. , and Sheeba K. . 2024. "Data Mining for Cyber Biosecurity Risk Management – A Comprehensive Review." Computers & Security 137: 103627. https://doi.org/https://doi.org/10.1016/j.cose.2023.103627.

Spirit of Asilomar Entreaty on Risks from Mirror life. 2025. "Risks from Mirror Life." Rice University Repository. https://repository.rice.edu/items/5ab21bd0-1574-43c5-a854-b4ac2b75d523 (Endorsed by 95+ participants from the February 2025 summit.).

Tyler, Dan, and Thiago Viana. 2021. "Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture." Applied Sciences (Switzerland) 11 (16). https://doi.org/10.3390/app11167499.

Wittmann, Bruce J., Tessa Alexanian, Craig Bartling, Jacob Beal, Adam Clore, James Diggans, Kevin Flyangolts, et al. 2025. "Strengthening Nucleic Acid Biosecurity Screening against Generative Protein Design Tools." Science 390 (6768): 82–87. https://doi.org/10.1126/SCIENCE.ADU8578;WEBSITE:WEBSITE:AAAS-SITE;JOURNAL:JOURNAL:SCIENCE;WGROUP:STRING:PUBLICATION.

World Health Organization. 2022. "Global Guidance Framework for the Responsible Use of the Life Sciences: Mitigating Biorisks and Governing Dual-Use Research." World Health Organization. 2022. https://www.who.int/publications/i/item/9789240056107.

Zafar, Sidra, Mohsin Nazir, Taimur Bakhshi, Hasan Ali Khattak, Sarmadullah Khan, Muhammad Bilal, Kim-Kwang Raymond Choo, Kyung-Sup Kwak, and Aneeqa Sabah. 2021. "A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things." IEEE Access 9: 93529–66. https://doi.org/10.1109/ACCESS.2021.3093442.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.