Cyberbiosecurity in Action: Securing the Biological Battlespace from Digital Subversion

Adya Daruka[1], Anusha Nigam[2] and Shreyas Kumar[3]
[1]University of Illinois Urbana Champaign, USA
[2]Centennial High School, Frisco, USA
[3]Texas A&M University, College Station, USA

adaruka2@illinois.edu
anusha.nigam.0101@gmail.com
shreyas.kumar@tamu.edu

Abstract: Cyberbiosecurity is an emerging discipline at the intersection of cybersecurity and life sciences, as digital dependence across genomics, laboratory automation, biomanufacturing, and digital health expands the attack surface of the bioeconomy. This paper synthesizes peer-reviewed literature, government reports, and public incident investigations to map cyber-biological threats, document observed incidents (e.g., healthcare ransomware and documented proofs-of-concept for DNA-encoded exploits), and identify systemic gaps in preparedness, workforce capacity, and governance. The literature indicates recurring vulnerabilities in healthcare and biotechnology supply chains, demonstrated operational impact from ransomware incidents, and credible research demonstrating new attack vectors such as malware encoded in synthetic DNA sequences. Drawing on these sources, we present the Integrated Cyberbiosecurity Defense Framework (ICDF) - a proposed multi-layered strategy combining bio-risk assessment, AI-driven detection, digital-twin simulation, fusion centers for cross-disciplinary response, and workforce development - and recommend policy, technical, and organizational steps for immediate adoption.

Keywords: Cyberbiosecurity, Biological battlespace, Bio-digital threats, Genomic data security, Synthetic biology cybersecurity, Digital health risk

1. Introduction

The convergence of biological research and digital technology has created new opportunities and vulnerabilities. As life sciences increasingly depend on computational methods, digital databases, and automated systems, they are exposed to cyber threats beyond the scope of traditional biosecurity. This fusion introduces risks that require urgent interdisciplinary attention, giving rise to the emerging field of cyberbiosecurity (Murch et al., 2018; Peccoud, 2018). Cyberbiosecurity focuses on protecting biological data, bioinformatics platforms, manufacturing systems, and healthcare technologies from threats such as hacking, ransomware, and espionage. Compromises in this domain can endanger intellectual property, public health, and national security. Yet, while cybersecurity and biosecurity have developed independently, their intersection remains underexplored. Cybersecurity frameworks rarely address the unique properties of biological data or the complexities of biotech infrastructure, while biosecurity practices focus largely on physical containment without integrating digital risks. This study addresses these gaps by examining cyberbiosecurity challenges across biotechnology, healthcare, and biomanufacturing. It identifies vulnerable assets, such as genomic databases and laboratory automation systems (Nix et al., 2021), and highlights low awareness among stakeholders and insufficient organizational preparedness. To respond, we propose a comprehensive framework combining policy development, cross-disciplinary collaboration, and workforce training. By illuminating vulnerabilities at the nexus of biology and cyberspace, this work emphasizes the urgent need for proactive strategies to secure the bioeconomy and build resilience in an increasingly digital life sciences sector.

2. Background

The digitization of biological research has fundamentally transformed life sciences, enabling faster discoveries, scalable bioengineering, and personalized healthcare. Genome sequencing, synthetic biology, and bioinformatics pipelines now rely almost entirely on digital platforms for storing, analyzing, and transmitting sensitive biological data. Unfortunately, this dependence introduces vulnerabilities that traditional biosecurity frameworks never anticipated. Genomic data presents unique challenges. Unlike typical personally identifiable information, genetic data is immutable and reveals extensive insights about individuals and entire populations. Breaches can compromise privacy, affect medical treatment and insurance decisions, and carry consequences that last for generations (Liu, 2019; Weiss, 2019). The shift toward cloud-based genomic platforms further amplifies risks of unauthorized access, data manipulation, and loss (Zhang and Wang, 2020).

Laboratory automation and biomanufacturing add another layer of cyber-physical risk. Robotics, IoT devices, and computer-controlled bioreactors improve efficiency but dramatically expand the attack surface for adversaries - from cybercriminals to nation-states (Kim, 2021; Li et al., 2021). Real-world incidents underscore these dangers: the 2017 WannaCry ransomware attack disrupted patient care across the UK's NHS (National Audit Office, 2018), while 2019 research demonstrated that malware could actually be encoded into DNA sequences (Ney et al., 2017; Brumfiel, 2020), blurring the line between biological and digital threats in disturbing ways. Policy responses remain fragmented. Agencies like HHS and DHS have issued sector-specific guidelines (U.S. Department of Health and Human Services, 2018; U.S. Department of Homeland Security, 2019), but no unified framework governs cyber risks in biology. Without standardized baselines, organizations rely on inconsistent, ad hoc measures.

Cultural barriers compound these technical challenges. Life scientists often lack cybersecurity training, while security professionals typically have limited understanding of biological workflows. Bridging this divide is essential. Cyberbiosecurity is not merely a theoretical concern - it represents an urgent operational necessity. This study synthesizes documented evidence of awareness gaps, preparedness challenges, and evolving threats across biotechnology, healthcare, and cybersecurity sectors while proposing concrete interventions to support resilient, scalable practices.

3. Related Work

Cyberbiosecurity, though a young discipline, has gained traction over the past decade. Early contributions by Murch et al. (2018) and Peccoud (2018) introduced the term and emphasized collaboration between cybersecurity experts and life scientists to protect biological assets. Subsequent work has mapped specific threats: Hu et al. (2020) showed how synthetic DNA ordering systems could embed malicious code, while Nix et al. (2021) highlighted risks in laboratory automation where compromised robots or sequencing tools could corrupt or steal data. Together, these studies underscore the seriousness of cyber risks in life sciences.

Healthcare cybersecurity research offers parallel insights. Hospitals have been frequent ransomware targets, with consequences for patient safety (Kruse et al. 2017). The rise of electronic health records has improved care but also created lucrative targets for data theft (Smith, 2018; Goodman, 2020). These findings demonstrate how disruptions in bio-related systems can carry life-threatening or economically significant consequences.Despite these advances, empirical studies on cyberbiosecurity awareness and preparedness remain limited. Most prior work is conceptual, focusing on hypothetical risks or technical fixes rather than stakeholder practices in biotechnology and healthcare. Current cybersecurity standards, including ISO/IEC 27001 and the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2020), offer general guidance but lack bio-specific controls, while biosecurity frameworks like the Federal Select Agent Program address physical hazards while overlooking digital threats. This regulatory gap reinforces the need for dedicated cyberbiosecurity policies.

Recent interdisciplinary workshops and whitepapers from organizations such as AAAS and DHS (U.S. Department of Homeland Security, 2019; Office of Science and Technology Policy, 2022) have called for cross-sector collaboration, but concrete models for integrating cybersecurity into biological research remain underdeveloped. This study extends the literature by synthesizing documented vulnerabilities and proposing a comprehensive framework that integrates cybersecurity, biosecurity, and organizational perspectives to strengthen resilience in the bioeconomy.

4. Methodology

This paper employs a systematic literature review and threat analysis methodology to synthesize the current state of cyberbiosecurity knowledge and propose a comprehensive defense framework. Our approach consisted of three phases:

Literature Collection. We conducted searches across peer-reviewed databases (PubMed, IEEE Xplore, Web of Science) and grey literature sources (government reports, white papers, technical documentation) using search terms including "cyberbiosecurity," "DNA malware," "laboratory automation cybersecurity," "healthcare ransomware," "bioeconomy safeguarding," and related phrases. We prioritized: (a) peer-reviewed research documenting cyber-biological attack vectors or defenses, (b) authoritative government reports on biosafety and cybersecurity, and (c) audited incident investigations from healthcare and biotechnology sectors.

Thematic Analysis. We extracted recurring themes from the literature including awareness gaps, supply-chain vulnerabilities, novel attack vectors, workforce deficits, and regulatory gaps. We analyzed documented incidents

(e.g., WannaCry NHS attack) and proof-of-concept research (e.g., DNA-encoded malware) to understand feasibility and impact of various threat scenarios.

Framework Development. Based on identified gaps and documented vulnerabilities, we synthesized findings into the Integrated Cyberbiosecurity Defense Framework (ICDF). This framework represents a conceptual architecture integrating best practices from cybersecurity, biosecurity, and risk management literature, adapted specifically for cyber-biological convergence challenges.

Limitations. This study is limited to publicly available literature and may be subject to publication bias. The rapidly evolving nature of cyberbiosecurity means new threats and defenses emerge continuously. The proposed framework has not been empirically validated and represents a theoretical contribution requiring future testing and refinement.

5. Results

Our review reveals several consistent themes across the cyberbiosecurity literature:

Awareness and Preparedness Gaps. Multiple policy reports and reviews document insufficient integration of bio-specific security measures into organizational information security programs. The National Academies' Safeguarding the Bioeconomy report highlights governance gaps and emphasizes the need for workforce development across life sciences and cybersecurity communities (NASEM, 2020). Peer-reviewed commentaries consistently identify a shortage of interdisciplinary training programs and professionals with both biological and cybersecurity expertise (Richardson et al., 2019).

Healthcare Incident Impact. Documented cyber incidents in healthcare demonstrate concrete operational harms. The 2017 WannaCry ransomware incident affecting the UK's NHS resulted in cancelled procedures, disrupted diagnostics, and prolonged service impacts (National Audit Office, 2018; Martin et al., 2017; Landi, 2019). European cybersecurity analyses document similar patterns across healthcare systems, illustrating how cyber incidents cascade into clinical harm (ENISA, 2021).

Supply-Chain Vulnerabilities. Cyberbiosecurity literature consistently identifies biological supply chains - including DNA synthesis providers, reagent vendors, outsourced laboratory services, and cloud bioinformatics platforms - as major systemic vulnerabilities where compromises can propagate through research and production pipelines (Richardson et al., 2019; ENISA, 2021).

Novel Attack Vectors. Experimental research demonstrates new classes of threats. Ney et al. (2017) demonstrated the conceptual feasibility of encoding exploit payloads into DNA sequences that, when processed by vulnerable bioinformatics pipelines, could trigger execution of malicious code. Additional research documents risks associated with compromised laboratory automation systems including robots and sequencers (Nix et al., 2021; Peccoud, 2018; Richardson et al., 2019).

Nation-State Targeting. Defense-oriented analyses indicate that intelligence communities view biological research infrastructure as strategic targets for espionage and capability theft (Murch et al., 2018; ENISA, 2021). Documented intrusion campaigns affecting research institutions and vaccine development programs illustrate this threat category.

Regulatory Gaps. Existing frameworks including the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2020) and HIPAA (U.S. Department of Health and Human Services, 2018) provide general control baselines but lack biology-specific controls for genomic database integrity, sequencing pipeline security, and synthetic biology platforms (NASEM, 2020; HHS, 2018).

Economic Impact. Incident investigations and sector assessments show that cyber incidents in health and biotechnology carry significant costs due to regulatory penalties, clinical disruption, and intellectual property loss (Martin et al., 2017; ENISA, 2021).

6. Findings

Based on our literature synthesis, we identify the following critical challenges that current cybersecurity approaches fail to adequately address:

6.1 Novel Threat Landscape

The literature documents a transformed threat environment where biological materials themselves can become cyber attack vectors. Research demonstrating DNA-encoded malware (Ney et al., 2017) represents a paradigm shift requiring new defensive approaches. Additionally, emerging AI capabilities in synthetic biology create new possibilities for both threat development and defense (Hu et al., 2020; Zhang and Wang, 2020).

6.2 Inadequate Bio-specific Controls

Organizations consistently lack security controls tailored to biological systems. Standard cybersecurity frameworks do not address unique challenges such as genomic data protection, synthetic biology platform security, or biomanufacturing resilience (Peccoud, 2018; Peccoud and Peccoud, 2020; NASEM, 2020).

6.3 Supply Chain as Attack Surface

The interconnected nature of biological research and manufacturing creates cascading vulnerability chains. Literature documents risks across DNA synthesis platforms, biological reagents, and research collaboration networks (Richardson et al., 2019; Berger, 2021).

6.4 Strategic Targeting

Government and defense analyses indicate that sophisticated actors increasingly target cyberbiosecurity assets, including genomic databases, vaccine research programs, and biodefense laboratories (Murch et al., 2018).

6.5 Regulatory Insufficiency

Current regulatory frameworks including HIPAA (U.S. Department of Health and Human Services, 2018), the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2020), and international biosecurity conventions do not adequately address cyber-biological convergence risks, creating uncertainty for organizations attempting compliance (Kruse et al., 2017; NASEM, 2020).

6.6 Workforce Deficits

Multiple sources identify cyberbiosecurity expertise as a critical capability gap. The interdisciplinary nature of required knowledge - spanning cybersecurity, biology, and policy - creates recruitment and training challenges. Literature documents systematic failures to develop cyberbiosecurity curricula in academic institutions (Richardson et al., 2019).

6.7 Technology Integration Challenges

Reviews note fundamental incompatibilities between traditional cybersecurity technologies and biological research environments. Legacy laboratory systems, specialized biological databases, and real-time bioprocess monitoring create unique security challenges that conventional tools cannot adequately address (Hu et al., 2020; Hardin, 2021; Miller, 2020).

6.8 Resource Requirements

Incident analyses suggest cyberbiosecurity breaches carry higher costs than traditional cybersecurity incidents due to regulatory penalties, intellectual property loss, and operational disruption (Martin et al., 2017; Landi, 2019; Smith, 2018). This necessitates greater investment in specialized expertise, technology, and processes.

7. Discussion

7.1 Framework Rationale

Our literature synthesis reveals that traditional cybersecurity approaches are insufficient for addressing cyber-biological convergence challenges. Current frameworks lack specialized controls for biological data protection, synthetic biology security, and biomanufacturing resilience (Murch et al., 2018; Richardson et al., 2019). The documented emergence of DNA-based attack vectors (Ney et al., 2017) and AI-augmented biological threats (Hu et al., 2020) represents a paradigm shift requiring purpose-built defensive strategies.We propose the Integrated Cyberbiosecurity Defense Framework (ICDF) as a multi-layered approach that addresses these unique challenges through six interconnected components designed to provide comprehensive protection across the biological domain.

7.2 Framework Components

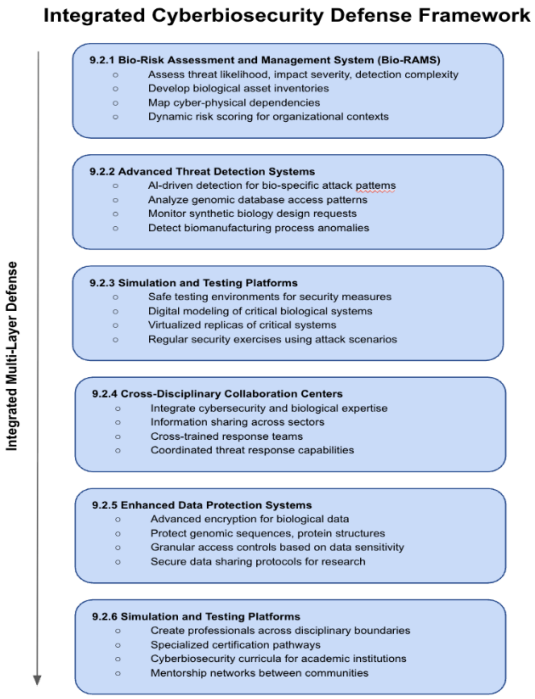

Figure 1: The Integrated Cyberbiosecurity Defense Framework (ICDF) showing six interconnected components for protecting biological systems from cyber threats

7.2.1 Bio-risk assessment and management system (Bio-RAMS)

Building on traditional risk assessment methodologies (NIST, 2020), Bio-RAMS extends these approaches to address cyber-biological threats specifically. This component assesses threat likelihood, impact severity, and detection complexity across genomic databases, synthetic biology platforms, and biomanufacturing systems. The system provides dynamic risk scoring adapted to organizational contexts and emerging threats.

Organizations should develop comprehensive biological asset inventories, map cyber-physical dependencies, and establish risk matrices accounting for both digital and biological consequences of security failures.

7.2.2 Advanced threat detection systems

Drawing on documented AI capabilities in threat detection (Hu et al., 2020), this component proposes specialized detection systems designed to identify bio-specific attack patterns. These systems analyze genomic database access patterns, synthetic biology design requests (Berger, 2021), and biomanufacturing process anomalies to identify potential attacks.

Deployment requires behavioral analytics tailored to biological workflows, baseline profiles for normal biological research activities, and alert mechanisms for anomalous patterns indicating potential compromise.

7.2.3 Simulation and testing platforms

This component develops safe testing environments for security measures without risking actual biological assets. Digital modeling of critical biological systems (Miller, 2020) enables organizations to evaluate security controls and incident response procedures in controlled settings.

In practice, organizations create virtualized replicas of critical systems, conduct regular security exercises using documented attack scenarios, and refine defenses based on simulation outcomes.

7.2.4 Cross-disciplinary collaboration centers

Addressing documented collaboration deficits (Richardson et al., 2019), this component establishes specialized centers integrating cybersecurity and biological expertise. These centers facilitate information sharing between biotechnology, healthcare, cybersecurity, and defense sectors while providing coordinated threat response capabilities.

Implementation requires establishing information sharing agreements, creating cross-trained response teams, developing common threat terminology, and conducting joint exercises across sectors.

7.2.5 Enhanced data protection systems

Recognizing the unique characteristics of biological data and long-term protection requirements, this component proposes advanced encryption and access control systems specifically designed for biological information including genomic sequences, protein structures, and bioinformatics workflows (Weiss, 2019; Zhang and Wang, 2020).

Organizations must implement strong encryption for biological data at rest and in transit, establish granular access controls based on data sensitivity, and develop secure data sharing protocols for research collaboration.

7.2.6 Workforce development program

This component addresses documented expertise gaps (Richardson et al., 2019) through comprehensive training initiatives creating professionals capable of operating across traditional disciplinary boundaries. The program includes specialized certification pathways, cross-training opportunities, and research collaboration mechanisms.

A practical approach involves developing cyberbiosecurity curricula for academic institutions, creating professional certification programs, establishing mentorship networks between cybersecurity and biological sciences communities (Peccoud and Peccoud, 2020), and supporting interdisciplinary research initiatives.

7.3 Implementation Roadmap

We propose a phased implementation approach spanning four years. Phase 1, covering the first twelve months, focuses on foundation building through organizational cyberbiosecurity assessments that identify current vulnerabilities and gaps. During this phase, organizations would develop comprehensive biological asset inventories cataloging genomic databases, laboratory automation systems, and biomanufacturing infrastructure. Baseline security controls would be established to address immediate risks, while workforce training programs would begin building internal expertise. The expected outcome of Phase 1 is basic cyberbiosecurity awareness across the organization and initial implementation of fundamental security controls.

Phase 2, spanning months 13 through 24, emphasizes capability development by deploying advanced detection systems tailored to biological workflows and attack patterns. Organizations would establish simulation environments for safe testing of security measures and incident response procedures without risking actual biological assets. This phase includes creating cross-sector collaboration mechanisms to enable information sharing with peer organizations in healthcare, biotechnology, and cybersecurity sectors. Enhanced data protection systems specifically designed for biological information (Weiss, 2019; Liu, 2019) would be implemented during this period. The expected outcome of Phase 2 is functional cyberbiosecurity capabilities with measurably improved threat detection and response times.

Phase 3, covering months 25 through 36, focuses on integration and optimization by bringing together all framework components into a cohesive defense system. Organizations would conduct comprehensive security exercises including red team assessments and simulated attack scenarios to test their integrated capabilities. Processes would be refined based on operational experience and lessons learned from exercises and real incidents. Workforce development programs would expand to build deeper expertise and create internal champions for cyberbiosecurity. The expected outcome of Phase 3 is a mature cyberbiosecurity program with coordinated defense capabilities across all organizational functions.

Phase 4, spanning months 37 through 48, develops advanced capabilities including deployment of automated response systems where appropriate to reduce response times for known threat patterns. Organizations would establish predictive threat intelligence capabilities (Choucri et al., 2019) to anticipate emerging risks before they manifest. Full cross-sector information sharing would be achieved, enabling real-time threat awareness across the broader community. Continuous improvement and adaptation mechanisms would be embedded to ensure the program evolves with the threat landscape. The expected outcome of Phase 4 is an advanced, adaptive cyberbiosecurity posture capable of addressing both current and emerging threats.

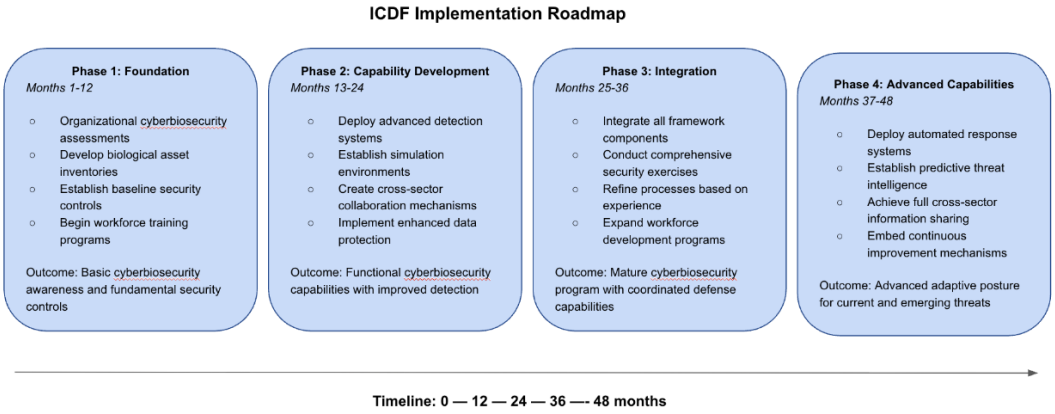

Figure 2: Four-phase implementation roadmap for deploying the ICDF over 48 months, from foundation building to advanced capabilities

7.4 Validation Requirements

The proposed framework requires empirical validation through multiple assessment approaches. Pilot implementations in diverse organizational contexts - academic research institutions, commercial biotechnology firms, healthcare facilities, and government laboratories - will test the framework's applicability across different operational environments. Red team exercises using documented attack vectors from the literature (Ney et al., 2017; Hardin, 2021) can evaluate the framework's effectiveness against known threats.

Longitudinal assessment of security improvements should track changes in vulnerability levels, incident frequency, and response effectiveness over extended periods. Cost-benefit analysis of implementation can quantify resource requirements against reduced incident risk and operational benefits. Finally, stakeholder feedback from biotechnology, healthcare, and cybersecurity sectors will ensure the framework addresses real-world needs and constraints faced by practitioners.

7.5 Expected Outcomes and Limitations

If successfully implemented, the ICDF framework should improve detection of cyber-biological threats through specialized monitoring systems attuned to biological workflow anomalies. The framework will enhance organizational preparedness through workforce development programs creating internal expertise spanning both cybersecurity and biological domains. Coordinated response capabilities will be enabled through cross-sector collaboration mechanisms facilitating rapid information sharing during incidents. Data protection will be strengthened through biology-appropriate controls designed specifically for genomic information and other sensitive biological data. Additionally, vulnerability to supply chain attacks should be reduced through enhanced vendor oversight and secure procurement processes for biological materials and services.

However, significant limitations exist. Implementation costs may be prohibitive for smaller organizations with limited cybersecurity budgets. Framework effectiveness depends on cross-sector cooperation that may prove difficult to achieve given competitive pressures and information sharing concerns in commercial biotechnology. The rapidly evolving threat landscape requires continuous framework adaptation, demanding ongoing investment and attention. Lack of empirical validation means actual performance metrics remain unknown until real-world testing occurs.

Success requires sustained organizational commitment and resource allocation over multiple years, which may be challenging to maintain through leadership changes and competing priorities. The framework represents a conceptual architecture requiring real-world testing, refinement, and validation. Organizations should adapt components to their specific contexts rather than attempting wholesale adoption without customization.

8. Conclusion

This literature synthesis establishes cyberbiosecurity as a critical emerging challenge requiring immediate attention across biotechnology, healthcare, and defense sectors. Our review demonstrates that traditional cybersecurity frameworks are insufficient for cyber-biological threats, particularly given documented incidents such as healthcare ransomware attacks (Landi, 2019; National Audit Office, 2018) and proof-of-concept research showing DNA-encoded malware as feasible attack vectors (Ney et al., 2017).

The proposed Integrated Cyberbiosecurity Defense Framework (ICDF) addresses these challenges through six components: Bio-Risk Assessment, Advanced Threat Detection, Simulation Platforms, Cross-Disciplinary Collaboration Centers, Enhanced Data Protection, and Workforce Development. This framework represents the first comprehensive architecture specifically tailored to biological systems and cyber-biological convergence.

Critical next steps include empirical validation through pilot implementations in healthcare, biotechnology, and research organizations to test the framework's practical applicability. The development of standardized cyberbiosecurity metrics is essential to enable consistent measurement and comparison of security postures across organizations. Establishment of regulatory guidance for cyber-biological risks would provide organizations with clear compliance requirements and reduce the current uncertainty around legal obligations. Investment in interdisciplinary workforce development programs is necessary to build the pipeline of professionals with combined expertise in cybersecurity and life sciences. Finally, creation of international cooperation mechanisms would enable coordinated threat intelligence sharing and response capabilities across national borders, recognizing that cyber-biological threats do not respect geographic boundaries. While implementation costs will exceed traditional cybersecurity programs, the documented impact of cyber incidents in healthcare and biotechnology - including operational disruption, intellectual property loss, and potential public health consequences - demonstrates the necessity of specialized defensive measures.

The convergence of AI, synthetic biology, and advancing cyber capabilities (Hu et al., 2020; Zhang et al., 2020; Yoo, 2020) creates unprecedented vulnerabilities extending beyond data breaches to potential manipulation of biological systems themselves. Regulatory frameworks (Office of Science and Technology Policy, 2022), educational programs, and international cooperation must evolve to meet this challenge.

Future research priorities include controlled testing of proposed framework components to validate their effectiveness in real-world settings. Longitudinal studies of threat evolution are needed to track how cyber-biological risks change over time and ensure the framework remains relevant. Researchers should develop validated effectiveness metrics that can objectively measure cyberbiosecurity improvements across different organizational contexts. Economic analysis comparing implementation costs against incident prevention benefits would help organizations justify investments in cyberbiosecurity programs. Finally, investigation of international governance mechanisms is essential to address the transnational nature of cyber-biological threats and enable coordinated global response capabilities. This paper provides a foundation for systematic cyberbiosecurity development, but practical validation and continuous adaptation remain essential. The biological domain's criticality to public health, food security, and economic stability makes effective cyberbiosecurity frameworks an urgent priority requiring sustained investment and cross-sector commitment.

Ethics Declarations: This work relies exclusively on published, publicly available literature, government reports, and audited incident investigations; no new human-subjects research, surveys, or interviews were conducted for this version of the analysis. Limitations include potential publication bias in incident reporting, the evolving nature of cyberbiosecurity threats (new technical capabilities and incidents may arise), and restricted availability of classified or private attribution details. Future work should complement the literature synthesis with structured primary research (surveys, interviews, and technical red-team exercises) if IRB approval and participant protections are obtained.

AI declaration: Artificial Intelligence tools were utilized in limited capacity during the development of this research paper for literature organization, reference formatting consistency, and editing support for clarity and professional presentation of complex technical concepts. The Integrated Cyberbiosecurity Defense Framework (ICDF) and its components represent novel conceptual contributions developed by the research team through systematic literature synthesis. All framework design, thematic analysis, and conclusions are the original intellectual work of the authors. AI tools were not used for literature selection, analysis interpretation, or generation of research conclusions. All content was verified for accuracy and originality by the authors.

References

Berger, M. (2021) 'The dark web and biotechnology risks', Nature Biotechnology, 39(4), pp.396–397. doi:10.1038/s41587-021-00896-8.

Brumfiel, G. (2020) 'DNA sequencing devices can be hacked', Nature, 579(7797), pp.16–17. doi:10.1038/d41586-020-00694-9.

Choucri, N., Madnick, S. and Ferwerda, J. (2019) 'Insiders and cybersecurity: Threats and countermeasures', Communications of the ACM, 62(2), pp.26–28. doi:10.1145/3303867.

ENISA (2021) Threat landscape for healthcare. Heraklion: European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications (Accessed: 2 October 2025).

Goodman, B. (2020) ‘Ethical challenges of digital health’, BMC Medical Ethics, 21(1), p.42. doi:10.1186/s12910-020-00478-4.
Hardin, J. (2021) ‘Securing bioinformatics pipelines: Threat modeling approaches’, Bioinformatics, 37(11), pp.1624–1631. doi:10.1093/bioinformatics/btaa883.
Hu, J., Gao, Y. and Liu, J. (2020) ‘Potential cybersecurity threats in synthetic biology’, Nature Communications, 11(1), p.3384. doi:10.1038/s41467-020-17102-9.
Kim, J. (2021) ‘Cyber resilience in healthcare IoT networks’, IEEE Internet of Things Journal, 8(12), pp.9512–9521. doi:10.1109/JIOT.2020.3048238.
Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K. (2017) ‘Cybersecurity in healthcare: A systematic review of modern threats and trends’, Technology and Health Care, 25(1), pp.1–10. doi:10.3233/THC-161263.
Landi, H. (2019) ‘Ransomware attacks in healthcare sector surged in 2019’, Healthcare IT News. Available at: https://www.healthcareitnews.com/news/ransomware-attacks-healthcare-sector-surged-2019 (Accessed: 2 October 2025).
Li, X., Zhang, Y. and Sun, Y. (2021) ‘Cyber-physical attacks and defenses in medical systems’, IEEE Transactions on Cybernetics, 51(9), pp.4564–4575. doi:10.1109/TCYB.2020.2985166.
Liu, L. (2019) ‘The future of genomic data privacy’, Trends in Genetics, 35(7), pp.429–431. doi:10.1016/j.tig.2019.04.001.
Martin, G., Ghafur, S., Kinross, J., Hankin, C., Darzi, A. and Jalil, R. (2017) ‘WannaCry: A year on’, BMJ, 361, k2381. doi:10.1136/bmj.k2381.
Miller, T. (2020) ‘Security issues in biomedical engineering’, Annual Review of Biomedical Engineering, 22, pp.459–483. doi:10.1146/annurev-bioeng-092019-030838.
Murch, R.S., So, W.K., Buchholz, W.G., Raman, S. and Peccoud, J. (2018) ‘Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy’, Frontiers in Bioengineering and Biotechnology, 6, p.39. doi:10.3389/fbioe.2018.00039.
National Academies of Sciences, Engineering, and Medicine (2020) Safeguarding the bioeconomy. Washington, DC: National Academies Press. doi:10.17226/25525.
National Audit Office (2018) Investigation: WannaCry cyber attack and the NHS. London: NAO. Available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ (Accessed: 2 October 2025).
National Institute of Standards and Technology (2020) Framework for improving critical infrastructure cybersecurity: Version 1.1 (NIST Special Publication 800-53 Rev. 5). Gaithersburg: NIST.
Ney, P., Koscher, K., Organick, L., Ceze, L. and Kohno, T. (2017) 'Computer security, privacy, and DNA sequencing: Compromising computers with synthesized DNA, privacy leaks, and more', in Proceedings of the 26th USENIX Security Symposium. Vancouver: USENIX Association, pp. 765–779.
Nix, R., Zhang, S., Tan, J. and Peccoud, J. (2021) ‘Cybersecurity risks in laboratory automation’, Nature Biotechnology, 39(8), pp.946–947. doi:10.1038/s41587-021-00970-1.
Office of Science and Technology Policy (2022) National security memorandum on strengthening biosecurity. Washington, DC: OSTP.
Peccoud, J. (2018) ‘Cyberbiosecurity: From naive trust to risk awareness’, Trends in Biotechnology, 36(1), pp.4–7. doi:10.1016/j.tibtech.2017.10.012.
Peccoud, J. and Peccoud, S. (2020) ‘Preparing for cyberbiosecurity: A policy framework’, Biotechnology Advances, 42, p.107592. doi:10.1016/j.biotechadv.2019.107592.
Richardson, L.C., Murch, R.S. and Peccoud, J. (2019) ‘Cyberbiosecurity: A call for cooperation in a new threat landscape’, Frontiers in Bioengineering and Biotechnology, 7, p.99. doi:10.3389/fbioe.2019.00099.
Smith, H.J. (2018) ‘Cybersecurity and data breaches: A growing public health concern’, American Journal of Public Health, 108(8), pp.989–990. doi:10.2105/AJPH.2018.304528.
U.S. Department of Health and Human Services (2018) Health industry cybersecurity practices: Managing threats and protecting patients (HICP Publication 405-D-0258). Washington, DC: HHS.
U.S. Department of Homeland Security (2019) Cyberbiosecurity: Next steps in securing the bioeconomy (DHS Publication 2019-CISA-01). Washington, DC: DHS.
Weiss, S. (2019) ‘Protecting biological data: Security measures in genome research’, Journal of Genomics and Informatics, 17(1), p.e7. doi:10.5808/GI.2019.17.1.e7.
Yoo, S. (2020) ‘Cyber threats in digital health innovation’, JMIR Medical Informatics, 8(2), p.e16725. doi:10.2196/16725.
Zhang, B. and Wang, H. (2020) ‘DNA data storage and its security challenges’, Frontiers in Bioengineering and Biotechnology, 8, p.581407. doi:10.3389/fbioe.2020.581407.
Zhang, Y., Deng, R.H. and Liu, Y. (2020) ‘Security and privacy in smart healthcare: Research challenges’, IEEE Internet of Things Journal, 7(5), pp.4424–4448. doi:10.1109/JIOT.2019.2942190.