From CPIS to CBISA: An Immune-Inspired Architecture for Bioeconomy-Scale Cyberbiosecurity

Babajide J. Asaju[1,2], Woosub Jung[2], Celisha Oscar[3], Lucas Potter[4] and Xavier-Lewis Palmer[4]
[1]Department of Defense Analysis, Naval Postgraduate School, Monterey, CA, USA
[2]Department of Computer and Information Sciences, Towson University, MD, USA
[3]Howard University, Washington, DC, USA
[4]BiosView Labs, Dayton, Ohio, USA

basaju@npsfoundation.org (Corresponding author)
basaju@towson.edu
biosview1@proton.me

Abstract: The digitization of biological research and production is creating increasingly interconnected cyber-physical environments spanning laboratory automation, genomic computation, biosensing, nucleic acid synthesis, and AI-enabled workflows. These systems require defenses that can respond not only to isolated cyber or biological threats, but also to risks that propagate across digital, physical, biological, and institutional boundaries. Foundational cyberbiosecurity scholarship established the importance of the biological–digital interface (Murch et al., 2018; Richardson et al., 2019), while immune-inspired cyber-physical models demonstrated distributed monitoring, adaptive detection, and self-healing principles in conventional CPS environments (Pang et al., 2021; Asaju et al., 2026). This paper proposes the Cyberbiosecurity Immune System Architecture (CBISA), a layered resilience framework that extends these principles across the bioeconomy through distributed sensing, cyber-physical monitoring, AI-assisted anomaly detection and assurance, data-integrity safeguards, lifecycle model controls, provenance, containment, and adaptive governance memory. The architecture is formalized through a hybrid risk evaluation function that combines biological impact, cyber-propagation, and dual-use factors, and through state-transition control logic linking detection, containment, recovery, and governance adaptation, illustrated with a worked biomanufacturing scenario. Drawing on intrusion detection, AI lifecycle security, synthesis screening, and data-governance scholarship (Siqueira et al., 2025; Meng and Zhang, 2025; Wheeler et al., 2024; Williamson et al., 2023), CBISA provides a cross-layer architecture for coordinated, bidirectional cyberbiosecurity defense across convergent bioindustrial systems.

Keywords: Cyberbiosecurity, Cyber-physical immune system, Bioeconomy, AI assurance, Adaptive governance, Nucleic acid Synthesis screening

1. Introduction

A foundation for integrated cyber-physical defense lies in cyber-physical systems (CPS) security, where contract-based design provides formal support for specifying and verifying system properties (Nuzzo et al., 2015), later extended toward compositional security guarantees (Sangiovanni-Vincentelli and Seshia, 2017); cross-layer approaches further show that cyber defense and resilient physical control should be designed jointly (Chen and Zhu, 2023). The complementary bio-inspired strand (Myakala, 2025) applies immunity to computer security. Artificial immune systems introduced self–nonself discrimination (Forrest et al., 1994), later extended by danger theory, in which responses follow signals of damage rather than foreignness alone (Aickelin and Cayzer, 2002; Kim et al., 2007). Pang et al. (2021) proposed the Cyber-Physical Immune System (CPIS), an overlay of distributed monitoring and system-level analysis modeled on innate and adaptive immunity, subsequently extended toward AI-supported self-healing, V2X, defense, and healthcare (Asaju et al., 2026), domains in which communication security remains an open challenge (Sivanantham et al., 2026). Immunosensor processes have also been modeled as CPS (Martsenyuk and Sverstiuk, 2019). These strands establish formal assurance, distributed monitoring, adaptation, and recovery, but were not designed to secure the bioeconomy as an integrated system.

Cyberbiosecurity addresses a convergence in which biological research and production depend on digital sensing, computation, and automation, so that cyber disruption can propagate into biological processes and biological artifacts can create digital risk (Murch et al., 2018; Richardson et al., 2019; Potter and Palmer, 2023; Naik et al., 2025). Recent work defines the field by whether cyber disruption produces measurable biological consequences (Pope, 2026a), and the convergence has been framed as a strategic security concern requiring coordination beyond conventional cybersecurity or biosecurity (George, 2019; Palmer and Karahan, 2020; Palmer, Potter and Karahan, 2020).

Existing controls address different portions of this attack surface. Nucleic-acid synthesis screening reduces misuse at the biological supply interface (Wheeler et al., 2024); lifecycle Bio-LLM safeguards address dataset, alignment, and inference risks (Meng and Zhang, 2025); and AI assurance is required where AI operates in high-

consequence infrastructure such as water and agricultural systems (Sobien et al., 2023). Comparative testing of GPT models against the FHIR healthcare standard found persistent limitations in accuracy, robustness, and trustworthiness, showing why domain-specific validation must precede high-stakes use (Pope and Patooghy, 2026). Governance work argues that policy enforcement should be separable from model inference and independently auditable (Palmer et al., 2026), while sovereignty-centered work warns that centralized architectures introduce concentration risks of their own (Perez et al., 2026). These approaches are complementary but do not yet form a unified resilience architecture. The need for integration is clearest at the interfaces. Ney et al. (2017) showed that synthesized DNA could exploit deliberately vulnerable downstream sequencing software, and structured non-executable content embedded in FASTA, CIF metadata, and protein sequences persisted through at least one stage in nine of ten modeled workflows (Pope, 2026b). Risk can therefore propagate through representations, pipelines, models, and decisions rather than remaining in a single layer. To address this gap, we propose the Cyberbiosecurity Immune System Architecture (CBISA), an immune-inspired resilience architecture that extends CPIS logic across biological, digital, physical, AI, and institutional layers. CBISA is explicitly bidirectional and combines adaptive anomaly detection with AI assurance, policy enforcement, provenance, containment, recovery, and governance memory, treating existing controls as specialized functions within a coordinated architecture rather than adding another isolated layer.

2. From CPIS to CBISA: Architectural PIllars and Scope Expansion

CPIS established distributed, immune-inspired monitoring and adaptive response in conventional CPS environments (Pang et al., 2021; Asaju et al., 2026), but was not designed around the requirements of bioeconomic systems: biological data as an adversarial substrate, bidirectional cyber–biological propagation, biological-consequence assessment, AI lifecycle assurance, and governance across organizational and jurisdictional boundaries (Potter and Palmer, 2023; Pope, 2026a; Pope, 2026b; Palmer et al., 2026). These requirements change the objects protected, the signals sensed, the consequences weighed during response, the authorities involved in escalation, and the information retained, so adding biological inputs to CPIS would not by itself suffice.

CBISA is organized around four pillars. Ecosystem-Scale Infrastructure shifts the unit of defense from an individual CPS to interdependent bioeconomic systems. Data as Security Surface treats biological data, metadata, and AI training or inference pipelines as attack surfaces (Ney et al., 2017; Pope, 2026b). Adaptive Governance couples detection and response with policy enforcement and institutional learning (Palmer et al., 2026; Perez et al., 2026), recognizing that policy frameworks for algorithmic systems must adapt continuously across technical and institutional levels (Asaju, 2026). Bidirectional Threat Propagation addresses both cyber-to-biological and biological-to-cyber pathways (Potter and Palmer, 2023; Pope, 2026a).

CBISA generalizes rather than replaces CPIS, retaining distributed observation, anomaly detection, adaptation, containment, and recovery while adding AI assurance, provenance, governance, and cross-layer coordination. Because defensive interventions can themselves impose biological, operational, or institutional costs, adaptation is treated as risk-aware rather than automatically beneficial (Weyns et al., 2025). Table 1 summarizes the key differences between CPIS and CBISA.

Table 1: Comparison of CPIS and CBISA architectural scope. CPIS provides the immune-inspired foundation for distributed monitoring, anomaly detection, adaptation, and mitigation, whereas CBISA extends this logic to the distinctive requirements of cyberbiosecurity, including bidirectional biological–digital threats, biological-data integrity, AI lifecycle assurance, consequence-aware response, and adaptive institutional governance. The distinction is therefore not simply one of scale, but of the objects protected, signals evaluated, responses authorized, and knowledge retained for future adaptation

Architectural dimension	Cyber-Physical Immune System (CPIS)	Cyberbiosecurity Immune System Architecture (CBISA)
Primary protected object	Cyber-physical systems and their interacting computational and physical components.	Interconnected biological, digital, physical, AI, and institutional systems across the bioeconomy.
Threat directionality	Primarily concerned with detecting and mitigating anomalous behavior affecting CPS operation.	Explicitly models both cyber-to-biological consequences and biological-to-cyber threat propagation.

Architectural dimension	Cyber-Physical Immune System (CPIS)	Cyberbiosecurity Immune System Architecture (CBISA)
Role of biological data	Biological data are not a primary security object in the original CPIS formulation.	Treats biological sequences, metadata, computational representations, provenance, and related data pipelines as security surfaces.
AI assurance	AI may support detection and self-healing in later CPIS extensions, but lifecycle AI assurance is not an intrinsic architectural function.	Treats AI as both a defensive capability and an object of assurance through provenance, model evaluation, adversarial testing, lifecycle safeguards, and policy controls.
Detection and analysis	Distributed monitoring and system-level anomaly analysis within CPS environments.	Extends distributed observation to cross-domain signal correlation involving biological processes, cyber infrastructure, AI systems, and institutional indicators.
Response logic	Adaptive mitigation and recovery directed toward maintaining CPS functionality and resilience.	Adds consequence- and risk-aware containment spanning digital, physical, biological, AI, and administrative responses, with escalation constrained by policy and authorization.
Memory and adaptation	Adaptive learning primarily supports improved technical detection and response.	Extends memory to include threat indicators, provenance, response outcomes, audit evidence, model safeguards, policy changes, and institutional learning.
Governance	Governance is not a principal internal architectural layer of the original CPIS model.	Incorporates governance as an adaptive architectural function linking detection, authorization, auditability, policy evolution, and cross-sector learning.
Scale and organizational scope	Originally demonstrated in bounded CPS settings, with later conceptual extensions to sectors including V2X, healthcare, and defense.	Designed for ecosystem-scale bioeconomic environments involving multiple organizations, supply chains, infrastructures, and potentially jurisdictions.
Architectural rationale	Provides the immune-inspired foundation of distributed sensing, adaptation, mitigation, and recovery.	Generalizes that foundation because bioeconomic security changes the protected objects, threat pathways, assurance requirements, response authorities, and forms of memory required for resilience.

3. Cyberbiosecurity Immune System Architecture

3.1 The Proposed CBISA Layered Architecture Consists of Four Coordinated Layers

CBISA organizes its defensive functions into four coordinated layers, shown in Figure 1.

The Innate Sensing Layer (Layer 1) provides continuous observation across biological, digital, physical, and AI-enabled environments, including biological data, laboratory telemetry, connected sensors, AI interfaces, and synthesis workflows (Pang et al., 2021; Asaju et al., 2026). Candidate mechanisms include schema and metadata validation, authenticated telemetry, device attestation, tamper-evident logging, and rule-based thresholds. In healthcare, network and physiological signals can be assessed jointly (Affia et al., 2023; Siqueira et al., 2025), with predictive physiological models providing a reference for detecting manipulated signals (Potter et al., 2024). The layer monitors both cyber-to-biological and biological-to-cyber risks.

The Adaptive Learning and Assurance Layer (Layer 2) correlates signals across layers to identify compound anomalies, supports risk scoring and adaptive thresholds, and protects datasets, model artifacts, and protocols through provenance tracking, dataset sanitization, adversarial testing, and lifecycle safeguards (Meng and Zhang, 2025; Pope, 2026b; Palmer et al., 2026). Federated approaches may support cross-organizational learning without centralizing sensitive biological data.

The Containment and Neutralization Layer (Layer 3) translates validated detection into proportionate response, such as artifact quarantine, credential revocation, model rollback, protocol suspension, synthesis restrictions, or supply-chain segmentation, extending the mitigation and self-healing logic of CPIS (Pang et al., 2021; Asaju et al., 2026). Response selection weighs biological and operational consequences rather than restoration speed alone.

The Governance Memory and Adaptation Layer (Layer 4) retains threat information, response outcomes, assurance findings, and policy changes through incident repositories, anomaly taxonomies, retraining triggers, and policy-version histories. Preventive controls such as synthesis screening contribute evidence to this memory, and new findings update subsequent screening and response rules (Wheeler et al., 2024), closing the adaptive feedback loop in Figure 1. Figure 2 illustrates the resulting response lifecycle.

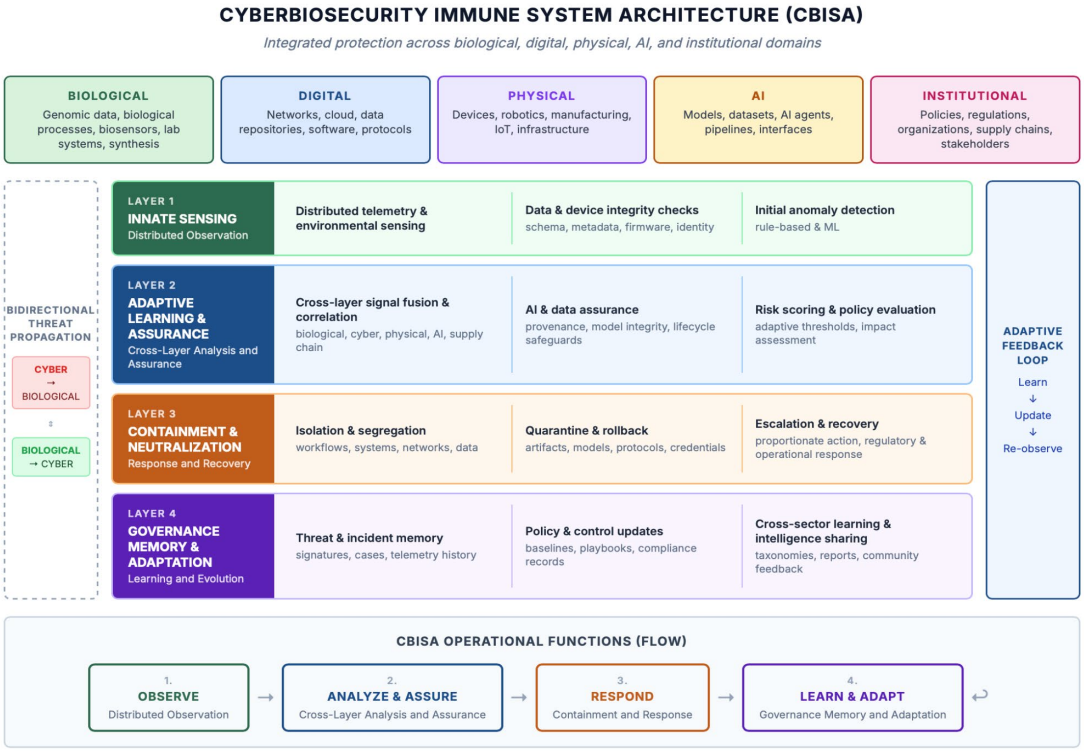

Figure 1: Cyberbiosecurity Immune System Architecture (CBISA). Four coordinated layers link distributed sensing, cross-layer analysis and assurance, containment, and governance memory across biological, digital, physical, AI, and institutional domains. The adaptive feedback loop enables incident knowledge and policy changes to inform subsequent detection and response, while bidirectional threat modeling addresses cyber-to-biological and biological-to-cyber propagation

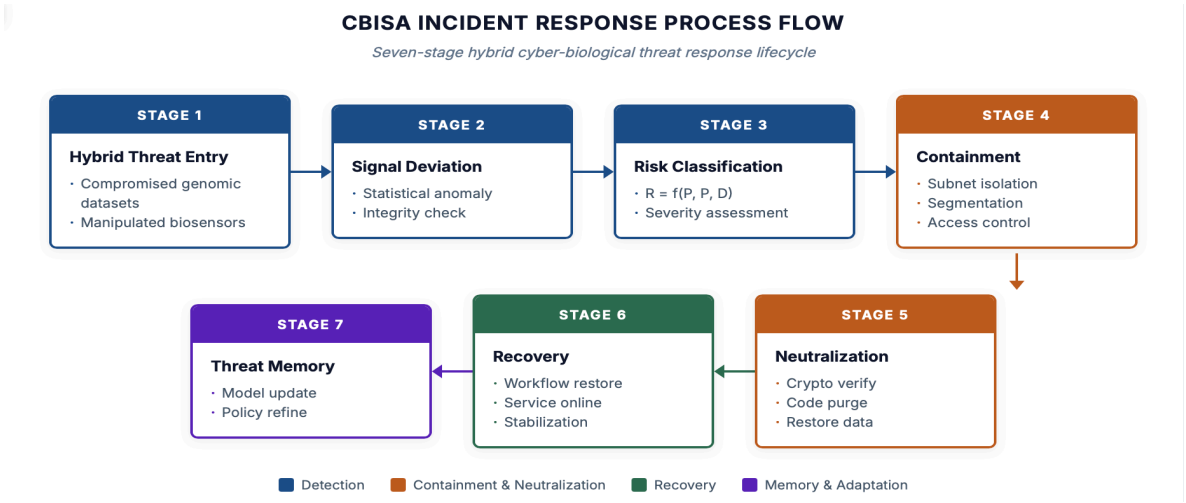

Figure 2: The seven-stage cyberbiosecurity immune response lifecycle. The lifecycle begins with hybrid threat entry (compromised genomic datasets or manipulated biosensor inputs), proceeds through bio-cyber signal deviation detection and hybrid risk classification, activates targeted containment and automated neutralization, ensures operational continuity and recovery, and culminates in hybrid threat memory for adaptive learning and policy refinement

3.2 Architectural Model of the Cyberbiosecurity Immune System

Table 1 establishes how CBISA extends CPIS (Pang et al., 2021; Asaju et al., 2026), and Figures 1 and 2 show its structure and incident lifecycle. The subsections that follow formalize the architecture through a system model, a hybrid risk evaluation function, and state-transition control logic.

3.3 System Model

For state-transition control, CBISA groups its environment into three coupled domains. The Biological Domain covers biological data, sequencing and synthesis workflows, clinical diagnostics, and biosurveillance. The Cyber-Physical Domain covers digital infrastructure, connected devices, automation, and AI-enabled systems. The Governance Domain covers authorization, sovereignty, dual-use oversight, auditability, and policy adaptation, reflecting convergent cyber, biological, and AI dual-use threats (Vaseashta, 2025). Cross-domain risk assessment, formalized in the hybrid risk evaluation function below, links the three domains.

3.4 Hybrid Risk Evaluation Function

CBISA evaluates convergent cyber-biological threats with a composite function $\mathbf{R} = f(\mathbf{P_{bio}}, \mathbf{P_{cyber}}, \mathbf{D_{dual}})$, where $\mathbf{P_{bio}}$ is the probability of biological impact (clinical harm, biomanufacturing interruption, or biosurveillance compromise), $\mathbf{P_{cyber}}$ is the cyber-propagation probability (lateral movement, network amplification, and cross-infrastructure spread), and $\mathbf{D_{dual}}$ is the dual-use amplification factor (potential for repurposing across research, commercial, or adversarial contexts). R prioritizes multi-domain response and informs recalibration in Layer 2. Figure 3 shows one candidate instantiation that combines weighted linear terms with a multiplicative interaction term, $R = \alpha \cdot P_{bio} + \beta \cdot P_{cyber} + \gamma \cdot D_{dual} + \delta \cdot (P_{bio} \times P_{cyber} \times D_{dual})$, and maps scores to CRITICAL, HIGH, MEDIUM, and LOW bands. The coefficients and thresholds are illustrative and require empirical calibration. The same function drives Stage 3 of Figure 2 and the escalation logic described in the next subsection.

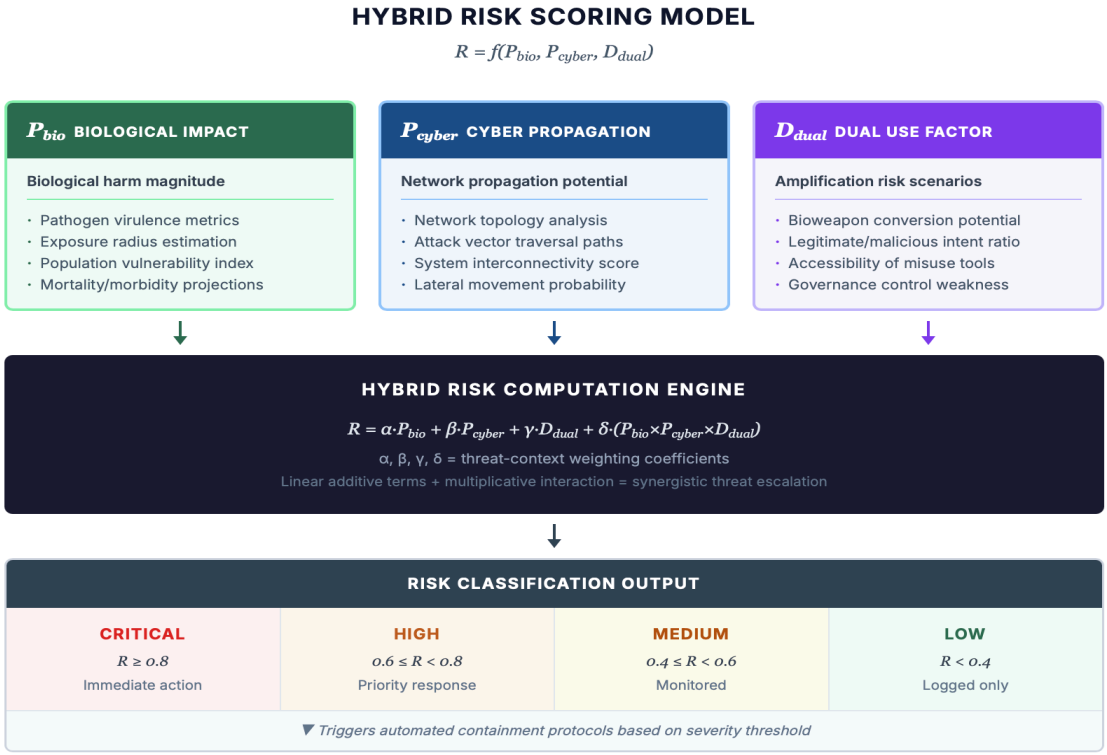

Figure 3: The three-layer computational architecture for hybrid cyberbiosecurity threat assessment. The input layer processes the composite factors of Pbio, Pcyber, and Ddual. The computation engine employs weighted linear and multiplicative transformations to derive normalized risk scores. The output layer translates these scores into categorical threat labels (CRITICAL, HIGH, MEDIUM, LOW), which dynamically initiate containment and neutralization protocols commensurate with the assessed risk level

3.5 State Transition Control Logic

The system begins in an Operational Baseline (S0) defined by validated telemetry, biological-data integrity, AI assurance status, and policy constraints. A material deviation moves it to Suspected Anomaly (S1), where cyber, biological, physical, AI, and supply-chain signals are correlated. A validated anomaly enters Threat Assessment (S2), where confidence, biological consequence, operational impact, and policy constraints are evaluated using the hybrid risk score R. Escalation is risk-aware rather than driven by anomaly magnitude alone (Weyns et al., 2025), paralleling danger-theory models in which response depends on evidence of harm (Aickelin and Cayzer, 2002).

Threats exceeding defined thresholds, such as the HIGH and CRITICAL bands in Figure 3, may trigger Containment (S3): network isolation, artifact quarantine, credential revocation, workflow suspension, model rollback, or synthesis restrictions, with high-consequence actions subject to predefined approval. Neutralization and Recovery (S4) includes integrity verification, provenance validation, model restoration, and staged workflow restoration; failed validation returns the system to S3. Confirmed incidents enter Governance Memory and Adaptation (S5), which updates detection rules, safeguards, thresholds, and governance controls, while false positives return to S0 with telemetry preserved. These states map to Figure 2: Stages 1–2 correspond to S0→S1, Stage 3 to S2, Stage 4 to S3, Stages 5–6 to S4, and Stage 7 to S5.

3.6 Design Implications and Scope

CBISA shifts the unit of protection to interconnected bioeconomic systems, couples detection with consequence-aware response, and embeds institutional learning in the resilience cycle. Several limitations apply. CBISA has not been implemented or empirically evaluated; P_{bio} and D_{dual} are difficult, and sometimes sensitive, to estimate, so the parameters in Figure 3 are illustrative; cross-organizational correlation creates tension with privacy and sovereignty that federated approaches reduce but do not eliminate (Perez et al., 2026); and automated containment risks false positives that disrupt legitimate work, which is why high-consequence responses require authorization. Simulation, testbed, and sector-specific pilot studies are needed (Figure 4).

4. Governance, Standards, and Sovereign Coordination

4.1 Governance of Synthesis Screening and Preventive Baselines

Sequence screening is a key preventive control at the digital-to-biological interface. Wheeler et al. (2024) propose a common international screening baseline, but differences among national requirements and provider practices may leave exploitable gaps, and practical questions about implementation and verification remain (Rose et al., 2024). Within CBISA, screening outcomes inform detection, provenance, and response, while new threats and audit findings update screening rules through governance memory. Sovereign coordination relies on interoperable minimum baselines, auditable screening, and controlled information exchange rather than centralized control, reducing regulatory arbitrage while preserving national and institutional authority.

4.2 AI Safety and Operational Governance

AI is both a defensive capability and a risk. AI-assisted intrusion detection and explainability support analysis and auditability (Siqueira et al., 2025), but misuse, compromised training data, adversarial inputs, and unreliable outputs require lifecycle controls such as dataset sanitization, runtime safeguards, and adversarial testing (Meng and Zhang, 2025). Policy controls should be independently specified and audited rather than embedded solely in model inference (Palmer et al., 2026), and governance of AI systems should integrate ethical, technical, and public-policy considerations within an adaptive framework (Asaju, 2026). Because AI reliability depends on well-curated, interoperable data (Williamson et al., 2023), evaluation results and incidents feed back into assurance thresholds and escalation procedures.

4.3 Cross-Sector Intelligence and Adaptive Governance Memory

Adaptive governance memory is the retention and reuse of validated incidents, audit findings, response outcomes, and policy changes through federated repositories, shared taxonomies, cross-sector exercises, and structured reporting, without centralizing sensitive data. Because centralization introduces dependency and loss-of-control risks (Perez et al., 2026), CBISA treats sovereignty and interoperability as complementary: institutions retain authority over data and policy while sharing enough assurance information to support collective defense.

5. Applications and Cross-Cutting Research Agenda

CBISA's core functions remain consistent across sectors, but implementation must reflect domain-specific hazards, data, regulation, and operational constraints. Figure 4 summarizes the resulting research agenda.

5.1 Healthcare and Biomedical Cyber-Physical Systems

Healthcare combines connected devices, physiological data, and AI-enabled decision systems (Affia et al., 2023; Asaju et al., 2026), amid substantial growth in ransomware attacks on care delivery (Neprash et al., 2022) and privacy concerns in bioinformatics–CPS integration (Shafik et al., 2025). Priorities include adversarially robust clinical AI, verified containment logic, and incident taxonomies linking cyber events to clinical consequences.

5.2 Environmental Biosurveillance and Water Infrastructure

Water and environmental systems involve sparse, noisy, and dispersed biological, chemical, and cyber signals (Sobien et al., 2023; Xiao et al., 2025). Priorities include secure telemetry, sensor trustworthiness, and cross-source anomaly correlation.

5.3 Agricultural and Plant Biotechnology Systems

Agriculture combines genomic data, AI-enabled analysis, and distributed infrastructure, with continuing data-standardization challenges (Williamson et al., 2023) and centralization risks (Perez et al., 2026). Priorities include adversarial testing of agricultural AI and governance that balances interoperability with local control.

5.4 Biomanufacturing and Synthesis Platforms

In biomanufacturing, digital actions directly produce biological outputs. CBISA could connect synthesis screening (Wheeler et al., 2024), provenance, process monitoring, and containment, recognizing that adversarial content can persist across computational workflows (Pope, 2026b). Priorities include digital-twin testbeds and formalized containment thresholds.

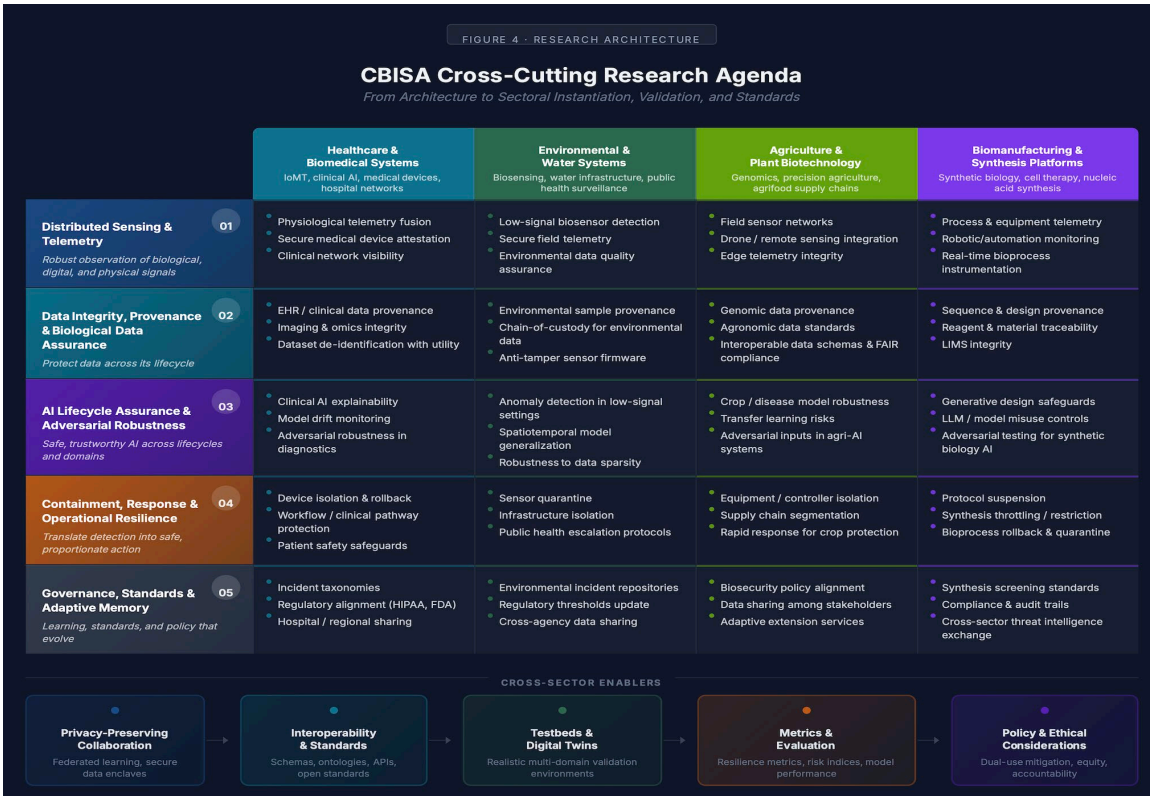

Figure 4: CBISA research gap matrix across key bioeconomic sectors. The matrix maps common research requirements in sensing, data integrity, AI assurance, containment, and governance to sector-specific challenges in healthcare, environmental and water systems, agriculture, and biomanufacturing. It highlights the empirical, technical, and institutional work needed to instantiate, evaluate, and govern the Cyberbiosecurity Immune System Architecture (CBISA) in real-world settings

5.5 Operational Example: CBISA in Biomanufacturing

Consider a synthesis workflow receiving a design with anomalous sequence or metadata characteristics. Layer 1 flags the deviation through schema, provenance, and screening checks. With illustrative weights $\alpha = 0.3$, $\beta = 0.2$, $\gamma = 0.2$, and $\delta = 0.3$ and initial estimates $P_{bio} = 0.7$, $P_{cyber} = 0.5$, and $D_{dual} = 0.8$, $R = 0.21 + 0.10 + 0.16 + 0.3 \times 0.28 = 0.554$ (MEDIUM), so the event is monitored in S2. Layer 2 then correlates the submission with anomalous activity on the submitting account, raising P_{cyber} to 0.9; R rises to approximately 0.701 (HIGH), moving the system to Containment (S3). Layer 3 suspends the workflow, quarantines artifacts, and restricts credentials while preserving unaffected operations. After recovery, Layer 4 records the incident, updates screening rules and thresholds, and preserves audit evidence. Cross-layer correlation thus changed the response although the biological signal did not, and the event updates future controls rather than only blocking a single request.

6. Conclusion

The digitization of the bioeconomy requires defenses for risks that cross biological, digital, physical, and institutional systems. CBISA links distributed observation, cross-layer analysis, containment, provenance, AI assurance, and governance memory within a coordinated resilience framework. As a conceptual foundation, it now requires formalization and empirical evaluation in real-world bio-industrial settings.

Acknowledgements

The authors thank Michaela Barnett, whose work in offensive security informed the framework used here, and whose feedback improved the final manuscript.

Ethics Declaration: An ethics declaration does not apply to this work.

AI Declaration: AI tools within Google Docs, ChatGPT, and Claude were used to assist with drafting, restructuring, formatting, reference checking, and figure re-design, under author direction. The authors remain responsible for the argument, source verification, final wording and all claims submitted for publication.

References

Affia, A.A.O., Finch, H., Jung, W., Samori, I.A., Potter, L. and Palmer, X.L. (2023) 'IoT health devices: Exploring security risks in the connected landscape', IoT, 4(2), pp. 150–182.

Aickelin, U. and Cayzer, S. (2002) 'The danger theory and its application to artificial immune systems', in Timmis, J. and Bentley, P.J. (eds.) Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS 2002). Canterbury, UK: University of Kent at Canterbury Printing Unit, pp. 141–148.

Asaju, B.J. (2026) The Dynamic Equity Framework Theory: A Global Model for Algorithmic Fairness and Cybersecurity Policy. Berlin/Boston: De Gruyter. ISBN: 9783112233283.

Asaju, B.J., Wakili, A.A., Guni, S. and Jung, W. (2026) 'The Cyber-Physical Immune System: A self-healing V2X framework for global defense and healthcare', Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026), 21(1), pp. 18–26. Reading, UK: Academic Conferences & Publishing International Limited. doi: 10.34190/iccws.21.1.4516.

Chen, J. and Zhu, Q. (2023) 'A cross-layer design approach to strategic cyber defense and robust switching control of cyber-physical wind energy systems', IEEE Transactions on Automation Science and Engineering, 20(1), pp. 624–635. doi: 10.1109/TASE.2022.3164860.

Forrest, S., Perelson, A.S., Allen, L. and Cherukuri, R. (1994) 'Self-nonself discrimination in a computer', in Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, pp. 202–212.

George, A.M. (2019) 'The national security implications of cyberbiosecurity', Frontiers in Bioengineering and Biotechnology, 7, Article 51. doi: 10.3389/fbioe.2019.00051.

Kim, J., Bentley, P.J., Aickelin, U., Greensmith, J., Tedesco, G. and Twycross, J. (2007) 'Immune system approaches to intrusion detection – a review', Natural Computing, 6(4), pp. 413–466. doi: 10.1007/s11047-006-9026-4.

Martsenyuk, V. and Sverstiuk, A. (2019) 'Cyber-physical model of the immunosensor system at the hexagonal lattice with the use of difference equations of the population dynamics', Сучасний стан наукових досліджень та технологій в промисловості, 1(7), pp. 75–84.

Meng, M. and Zhang, Z. (2025) 'A biosecurity agent for lifecycle LLM biosecurity alignment', arXiv, arXiv:2510.09615. doi: 10.48550/arXiv.2510.09615.

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, Article 39. doi: 10.3389/fbioe.2018.00039.

Myakala, P.E. (2025) 'A bio-inspired paradigm for computational intelligence', Journal of Artificial Intelligence and Big Data, 5(1), pp. 10–31586.

Naik, N. et al. (2025) 'When cybersecurity becomes cyberbiosecurity: Understanding cyberbiosecurity, its principles, components, importance, and challenges', in The International Conference on Computing, Communication, Cybersecurity & AI (C3AI 2025).

Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., Rozenshtein, A.Z. and Nikpay, S.S. (2022) 'Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021', JAMA Health Forum, 3(12), e224873.

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 26th USENIX Security Symposium (USENIX Security 17), pp. 765–779.

Nuzzo, P., Sangiovanni-Vincentelli, A.L., Bresolin, D., Geretti, L. and Villa, T. (2015) 'A platform-based design methodology with contracts and related tools for the design of cyber-physical systems', Proceedings of the IEEE, 103(11), pp. 2104–2132. doi: 10.1109/JPROC.2015.2453253.

Palmer, X.L. and Karahan, S. (2020) 'Defending forward: An exploration through the lens of biocybersecurity', in ICCWS 2020: 15th International Conference on Cyber Warfare and Security. Reading, UK: Academic Conferences and Publishing International Limited, p. 373.

Palmer, X.-L., Potter, L. and Karahan, S. (2020) 'On the emerging area of biocybersecurity and relevant considerations', in Arai, K., Kapoor, S. and Bhatia, R. (eds.) Advances in Information and Communication. Cham: Springer, pp. 873–881. doi: 10.1007/978-3-030-39442-4_66.

Palmer, X.L., Potter, L., Lesaja, L., Karathanasis, S.K. and GhasemiGol, M. (2026) 'Biosecure-LLM framework: Protecting LLMs from cyberbiosecurity threats and the case for independent AI safety governance', Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026), 21(1), pp. 743–750. Reading, UK: Academic Conferences and Publishing International Limited. doi: 10.34190/iccws.21.1.4524.

Pang, B., Verma, A., Zhou, J., Incer, I. and Sangiovanni-Vincentelli, A. (2021) 'Work-in-progress: The Cyber-Physical Immune System', in 2021 International Conference on Embedded Software (EMSOFT), pp. 43–44. doi: 10.1145/3477244.3477621.

Perez, R., Palmer, X., Potter, L., Hattoh, D.K., Addo, S.A. and Lesaja, S. (2026) 'From surveillance monocultures to agroecological defense: A sovereignty-centered framework for agricultural cyberbiosecurity', Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026), 21(1), pp. 355–364. Reading, UK: Academic Conferences & Publishing International Limited. doi: 10.34190/iccws.21.1.4544.

Pope, T. (2026a) 'Defining cyberbiosecurity by biological consequence', Proceedings of the 47th IEEE Symposium on Security and Privacy Workshops (SPW 2026), pp. 214–220. doi: 10.1109/SPW72489.2026.00025.

Pope, T. (2026b) 'Sleeper code in protein data files as cyber adversarial vectors', Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026), 21(1), pp. 624–632. Reading, UK: Academic Conferences & Publishing International Limited. doi: 10.34190/iccws.21.1.4459.

Pope, T. and Patooghy, A. (2026) 'Comparative evaluation of GPT models in FHIR proficiency', ACM Transactions on Intelligent Systems and Technology, 17(4), Article 83, pp. 1–25. doi: 10.1145/3718095.

Potter, L. and Palmer, X.L. (2023) 'Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination', in Greenbaum, D. (ed.) Cyberbiosecurity: A New Field to Deal with Emerging Threats. Cham: Springer, pp. 37–69. doi: 10.1007/978-3-031-26034-6_4.

Potter, L., Shetty, S., Karahan, S. and Palmer, X.L. (2024) 'Biocybersecurity and applications of predictive physiological modelling', International Journal of System of Systems Engineering, 14(4), pp. 349–361.

Richardson, L.C., Connell, N.D., Lewis, S.M., Pauwels, E. and Murch, R.S. (2019) 'Cyberbiosecurity: A call for cooperation in a new threat landscape', Frontiers in Bioengineering and Biotechnology, 7, Article 99. doi: 10.3389/fbioe.2019.00099.

Rose, S., Alexanian, T., Langenkamp, M., Cozzarini, H. and Diggans, J. (2024) 'Practical questions for securing nucleic acid synthesis', Applied Biosafety, 29(3), pp. 159–171.

Sangiovanni-Vincentelli, A.L. and Seshia, S.A. (2017) CPS: Medium: Quantitative Contract-Based Synthesis and Verification for CPS Security. NSF Award 1739816. National Science Foundation, University of California, Berkeley. Available at: https://ui.adsabs.harvard.edu/abs/2017nsf....1739816S/abstract (Accessed: 28 February 2026).

Shafik, W. et al. (2025) 'Ethical and privacy concerns in bioinformatics and cyber-physical systems integration in healthcare', in AI-Driven Personalized Healthcare Solutions, pp. 333–364.

Siqueira, L.P., Batista, C.L., Lui, P.H., Kazienko, J.F., Quincozes, S.E., Quincozes, V.E., Welfer, D. and Nomura, S. (2025) 'A comprehensive survey on intrusion detection systems for Healthcare 5.0: Concepts, challenges, and practical applications', Sensors, 25(20), Article 6261.

Sivanantham, T. et al. (2026) 'Securing Vehicle-to-Everything (V2X) communication: Challenges, mechanisms, and future directions', Wireless Personal Communications, pp. 1–107.

Sobien, D., Yardimci, M.O., Nguyen, M.B., Mao, W.Y., Fordham, V., Rahman, A., Duncan, S. and Batarseh, F.A. (2023) 'AI for cyberbiosecurity in water systems—A survey', in Greenbaum, D. (ed.) Cyberbiosecurity: A New Field to Deal with Emerging Threats. Cham: Springer, pp. 217–263. doi: 10.1007/978-3-031-26034-6_13.

Vaseashta, A. (2025) 'Developing resilience against cyber, chemical, biological, and artificial intelligence dual-use technology threats', in Multidisciplinary International Conference of Research Applied to Defense and Security, pp. 11–24.

Weyns, D. et al. (2025) 'An architectural viewpoint for benefit-cost-risk-aware decision-making in self-adaptive systems', ACM Transactions on Autonomous and Adaptive Systems, 20(1), pp. 1–65. doi: 10.1145/3705612.

Wheeler, N.E., Carter, S.R., Alexanian, T., Isaac, C., Yassif, J. and Millet, P. (2024) 'Developing a common global baseline for nucleic acid synthesis screening', Applied Biosafety, 29(2), pp. 71–78. doi: 10.1089/apb.2023.0034.

Williamson, H.F., Brettschneider, J., Caccamo, M., Davey, R.P., Goble, C., Kersey, P.J., May, S., Morris, R.J., Ostler, R., Pridmore, T. and Rawlings, C. (2023) 'Data management challenges for artificial intelligence in plant and agricultural research', F1000Research, 10, Article 324.

Xiao, Y., Du, Z., Li, Y., Cao, L., Zhu, B., Kitaguchi, T. and Huang, C. (2025) 'A review on the application of biosensors for monitoring emerging contaminants in the water environment', Sensors, 25(16), Article 4945.