From Surveillance Monocultures to Agroecological Defense: A Sovereignty-Centered Framework for Agricultural Cyberbiosecurity

Rolando Perez[1], Xavier Palmer[2], Lucas Potter[2], Dodzi Koku Hattoh[3], Salomey Afua Addo[4], and Srdjan Lesaja[5]

[1]Blue Marble Space Institute of Science, Seattle, WA, USA
[2]BiosView Labs, Dayton, Ohio, USA
[3]University of Ghana, Accra / Bonn Sustainable AI Lab, Bonn, Germany
[4]University of Cambridge, UK

rolando.perez@bmsis.org

Abstract: Agricultural cyberbiosecurity (CBS) scholarship may have overwhelmingly adopted centralized, national-security-oriented frameworks that leave community-governed and agroecologically-grounded alternatives unexplored. Recent AI safety research casts doubt on the viability of general-purpose, centralized safety regimes versus bounded or decentralized ones (Panigrahy and Sharan, 2025). Some leading proponents of centralized CBS paradigms propose surveillance architectures spanning unified biological intelligence (BIOINT), national bioaudit systems, and coordinated governance bodies that may cost billions of dollars. Centralized approaches often compellingly diagnose monoculture vulnerabilities, biosurveillance urgency, and the need for novel governance mechanisms. However, in these centralized architectures, communities receive biosecurity services but do not co-govern biosurveillance priorities, data use, or safety specifications, and agriculture remains a critical infrastructure to be defended from above. Even when such centralized paradigms propose distributed biological sensing, such as engineered sentinel plants and living biosensors, these systems require routine community-level care, maintenance, and trust relationships that centralized architectures cannot deliver, and will demand iterative updating as threat landscapes evolve. The empirical record confirms the costs of centralization: millions in ransom paid by JBS and a considerable percentage of U.S. grain production disrupted by a single cooperative's software failure (Yazdinejad et al., 2021; Cartwright and Cartwright, 2023). Coordination gaps are real, and new institutions are necessary to address them. However, coordination without corresponding community-level governance authority reproduces the monoculture pattern at the institutional level. This paper argues that agricultural defense must be rooted in the slowest and most durable layers of change identified by Stewart Brand's pace-layer framework: nature and culture. We advance three interlocking components: (1) agroecology as defensive architecture, in which biological diversity and functional redundancy constitute the primary cyberbiosecurity strategy; (2) sovereignty-preserving biosurveillance, in which community-governed federated sensing networks retain local data authority while enabling collective threat detection through privacy-preserving mechanisms; and (3) cooperative assurance from below, in which safety specifications are collectively deliberated and verified through participatory guarantee systems rather than centralized certification hierarchies (Dalrymple et al., 2024; Carroll et al., 2020; Manoj et al., 2025). This framework does not preclude centralized pathogen detection when necessary, but insists that top-level and community-level institutions be in relation with one another so that coordination flows bidirectionally rather than exclusively from above. Rather than claiming comprehensive safety guarantees, we demonstrate how bounded formal assurances, when integrated with agroecological resilience and community governance, can materially improve the security of food systems under real-world constraints.

Keywords: Biosecurity; Biofutures; Stewardship, Sovereignty, AI, Indigenous Data Governance

1. Introduction: Two Architectures for Agricultural Defense

As agriculture integrates artificial intelligence, networked sensors, and advanced biotechnologies, new risks emerge alongside potential benefits. AI models that optimize drone irrigation can be manipulated through data poisoning to trigger drought stress; botnets of compromised agritech devices could incapacitate farm networks during critical harvest windows (Aldhyani and Alkahtani, 2023; Pasca et al., 2025). Such disruptions cascade across food supply chains, amplify biosecurity incidents, and erode trust in markets and governance institutions (Duncan et al., 2019; Drape et al., 2021).

The cyberbiosecurity (CBS) discipline emerged to address convergent risks at the interface of biological systems, digital infrastructure, and national security. Foundational work by Murch et al. (2018) framed CBS around protecting the bioeconomy and mitigating national security threats, a paradigm extended by George (2019) through nuclear-deterrence analogies and reinforced in subsequent scholarship (Duncan et al., 2019; Stephen et al., 2023; Greenbaum, 2023). Recent CBS-adjacent policy-oriented contributions continue this orientation, advancing proposals for integrated biological intelligence systems, bioaudit mechanisms modeled on financial oversight, and expanded federal coordination structures (National Academies of Sciences, Engineering, and Medicine, 2018; Knight and Sureka, 2024; Endy et al., 2025). These proposals typically frame biology as an open, distributed network while advocating centralized architectures for biosurveillance, verification, and governance. At the same time, the literature makes substantive contributions, including articulating novel verification

mechanisms, emphasizing monoculture vulnerability, and situating biological security within long-term global food and supply-chain dependencies.

We support the view that coordination gaps are real. In the United States, fragmented biosecurity authority across multiple agencies may have historically hindered threat detection and response, and a new federal coordinating capacity is necessary. Centralised coordination that lacks corresponding community-level governance authority risks reproducing monoculture dynamics at the institutional level, consolidating surveillance, certification, and decision-making within a single hierarchical framework rather than distributing oversight across diverse local actors (Jannah et al., 2025; Powell et al., 2021). This paper argues that the top-level institutions needed must be in relation with community-level governance institutions, cooperative data governance bodies, participatory assurance networks, and farmer-led biosurveillance, so that coordination flows bidirectionally rather than exclusively from above.

Security is not synonymous with safety. Highly surveilled agricultural systems may be secured against external threats while remaining unsafe for farmers and ecosystems due to loss of autonomy, repair rights, and democratic oversight (Drape et al., 2021). The remainder of this paper examines the centralization paradox through the empirical cyberattack record (Section 2), establishes theoretical bounds on AI safety guarantees (Section 3), presents agroecology as defensive architecture (Section 4), develops a sovereignty-centered governance alternative (Section 5), models competing threat prioritizations (Section 6), and concludes with implementation pathways and limitations (Section 7).

2. A Centralization Paradox in CBS

Cyberbiosecurity analyses characterise agricultural cybersecurity as a collective-action problem shaped by fragmented ownership structures and uneven capacity, resulting in underinvestment in system-wide protection across interconnected supply chains (Duncan et al., 2019; Drape et al., 2021). Duncan et al. (2019) contend that agricultural cybersecurity suffers from a collective-action problem, as firms lack incentives to secure shared networks, and that the sector's diversity limits the effectiveness of centralized governance models (Duncan et al., 2019). Drape et al. (2021) report from a ~170-participant workshop that no group represented in the discussions had access to cybersecurity training or resources, highlighting widespread gaps in workforce preparedness and awareness around cyberbiosecurity across sectors, rather than evidence of training penetration at the farm level specifically. Greenbaum's (2023) comprehensive volume includes a chapter on safeguarding against social injustices, yet the CBS canon by and large remains institutional, bioeconomy-oriented, and state-centric. Across this literature, no work appeared to systematically address farmer data sovereignty, agroecological systems, community self-governance for security, or the risk that CBS frameworks themselves become instruments of surveillance and corporate consolidation.

Emerging biosecurity frameworks describe a distributed biological sensing network integrating routine antibody repertoire monitoring, bioengineered environmental sentinels, and real-time genomic sequencing, framing continuous bio-detection capacity as essential to national resilience against rapidly evolving or covert biological threats (Knight and Sureka, 2024; Endy et al., 2025). Concentrating detection, analysis, and response authority within a unified system reduces institutional diversity and increases systemic coupling, a structural condition that some cyberbiosecurity analyses identify as heightening vulnerability in tightly integrated agricultural and food system infrastructures (Peccoud et al., 2018; Murch et al., 2018). The proposed response, BIOINT, is to scale the same architectural logic rather than question it. BIOINT exemplifies the centralization paradox at its most ambitious scale. The proposed BIOINT architecture describes continuous, multi-domain metagenomic surveillance across environmental, agricultural, and human systems, coupled with cross-agency data integration and AI-enabled analytics to accelerate detection and attribution of emerging biological threats (Knight and Sureka, 2024; Endy et al., 2025).

The empirical record of agricultural cyberattacks reinforces the case that centralization can be a primary vulnerability. Ransomware activity in the food and agriculture sector demonstrates how attackers exploit centralized digital platforms and time-critical operations to generate disproportionate downstream effects across consolidated supply chains, preferentially timing intrusions to periods of heightened operational pressure such as planting, harvest, or peak processing windows (Cartwright and Cartwright, 2023; Yazdinejad et al., 2021). These risks are amplified by structural consolidation, which creates single points of failure whose compromise can affect substantial portions of production simultaneously (Perrow, 1999; Boyson, 2014; Ashley et al., 2022). The vulnerability profile of network-connected agricultural equipment makes this concrete. Across DEF CON 29 and DEF CON 30, security researcher Sick Codes demonstrated how weak defaults, exposed administrative interfaces, outdated operating systems, and insecure remote-management features in John Deere and related

platforms could enable high-privilege access to centralized operations systems and, by extension, large fleets of connected equipment (Sick Codes, 2021; Sick Codes, 2022). Complementary assessments identified more than 100 distinct vulnerabilities in Deere's corporate networks during a 10-day white-hat engagement (Manglicmot, 2022). Cyberbiosecurity scholarship has noted that software-locked agricultural machinery concentrates control over repair, modification, and operation within OEM ecosystems, and proprietary diagnostic restrictions further exacerbate exposure by preventing equipment owners from detecting or remediating vulnerabilities independently, thereby entrenching both risk and dependency (Wiens, 2018; Gambino, 2023; Stephen et al, 2023).

Cyberbiosecurity scholarship increasingly treats large-scale monoculture dominance, concentrated animal feeding operations, and globally interdependent food trade networks as structural amplifiers of systemic vulnerability, as agricultural uniformity reduces ecological resilience, intensification increases zoonotic emergence risk, and trade coupling enables cascading disruption (Altieri, 2009; Jones et al., 2013; Puma et al., 2015; Stephen et al, 2023). Yet some CBS experts and adjacent practitioners treat these exclusively as infrastructure problems requiring top-down monitoring and federal intervention. Farmers appear primarily as reluctant subjects of biosurveillance, never as active biosecurity agents whose knowledge, practices, and governance capacity constitute a defensive resource. The word "sovereignty" appears insufficiently in the CBS literature in an agricultural context. A recent biotechnology governance proposal utilises Society Readiness Levels to assess societal preparedness alongside technological maturity, noting that readiness varies across stakeholder groups and may be more decisive than technical development alone (Endy et al., 2025). This framework path offers a valuable lens that could be applied more broadly, including to CBS governance proposals themselves. For instance, the societal readiness of persistent metagenomic surveillance among the agricultural and Indigenous communities these systems would engage is likely low. Here, the SRL framework itself suggests a design insight worth further development: when societal readiness is low, and architecture depends on community participation, noncompliance becomes a systemic biosecurity vulnerability, not a problem of public education but a structural signal warranting alternative design approaches. Cyberbiosecurity is a necessary but insufficient component of agricultural defense. The centralization paradox is not that centralized capacity is unnecessary; it is that centralization unaccompanied by distributed capacity and governance authority converts a defensive architecture into a single point of failure. The following section examines why the AI safety literature reinforces this conclusion.

3. Bounded Assurance: What Safety Can and Cannot Guarantee

Panigrahy and Sharan (2025) prove an impossibility result showing that no AI system can simultaneously satisfy strong notions of safety, trust, and full generality. Drawing an analogy to Gödel's incompleteness theorems, they argue that safety- and trust-constrained systems must exclude some task instances that fall within the scope of general human problem-solving. The authors explicitly note that this result motivates the use of weaker, practical interpretations of safety and trust in real-world deployments.

Tegmark and Omohundro (2023) propose one of the most ambitious centralized safety architectures in the AI safety literature, advocating a hierarchy of provably compliant systems spanning software, hardware, and contractual enforcement mechanisms. Yet their concrete examples of tractable specifications, such as restricting DNA synthesizers from producing certain pathogens or imposing geofencing and time limits on AI hardware, appear to remain narrowly bounded rather than universal. Zero-knowledge proofs for DNA synthesis screening allow researchers to cryptographically verify that a requested sequence does not appear on a prohibited list without revealing the sequence itself, a genuinely useful application of privacy-preserving verification to a discrete and formally specifiable task. However, bounded systems address the verification problem without addressing the governance problem: who defines which sequences are dangerous, who maintains the reference database, and who decides the detection thresholds. Privacy-preserving verification without governance over the standards being verified is technical sophistication in the service of unexamined authority. Moreover, practitioners seem to confine this privacy-preserving logic to a single commercial checkpoint while deploying AI throughout BIOINT's analytical layer as an unconstrained force multiplier, without engaging whether this introduces the systemic vulnerability precisely of the kind Panigrahy and Sharan identify. Cryptographic privacy is offered to those with intellectual property to protect; pervasive data collection with "anonymized" and "opt-in" mentioned only in passing is proposed for everyone else.

Dalrymple et al. (2024), representing a broad coalition of AI safety researchers, articulate the Guaranteed Safe AI paradigm through three components: a world model, a safety specification, and a verifier. Their framework recognizes a spectrum of assurance mechanisms from formal proofs to probabilistic guarantees and empirical testing. Crucially, they emphasize that safety specifications must encode societal risk criteria and should ideally

be informed by collective deliberation, not solely as a technical problem but as a governance challenge. Their proposal for compositional verification, in which complex systems are decomposed into independently verified modules, points toward a distributed architecture of assurance. In agricultural cyberbiosecurity, different components may warrant distinct assurance regimes, ranging from formal verification in bounded control systems to empirical validation in complex agroecological monitoring.

Tomašev et al. (2025) advance a more radical departure by proposing distributional AGI safety, in which general intelligence emerges from the coordination of many specialized agents rather than a single monolithic system. Their framework emphasizes institutional and incentive-based controls, including reputation systems, cryptographic identity, and anti-monopoly safeguards, rather than universal internal alignment. This perspective maps naturally onto agricultural technology ecosystems, where safety and resilience emerge from interactions among heterogeneous tools, actors, and governance structures that eliminate reliance on centralized verification alone.

Collectively, these four contributions establish that complete safety is impossible (Panigrahy and Sharan, 2025), ambitious but practically limited to bounded applications (Tegmark and Omohundro, 2023), best understood as a spectrum requiring collective deliberation (Dalrymple et al., 2024), and most effectively achieved through distributed governance rather than monolithic control (Tomašev et al., 2025). Bounded examples from leading CBS paradigms, DNA synthesis screening, and geofenced hardware point toward this conclusion even as their overall architecture moves in the opposite direction. Agricultural AI safety requires bounded, task-specific, formally constrained subsystems, governed through collective deliberation, rather than comprehensive guarantees imposed over socio-ecological complexity.

4. Agroecology as Defensive Architecture

Agroecological systems, characterized by biodiversity, soil health, decentralization, and local knowledge, reduce biological, ecological, and cyber-biological vulnerabilities by design (Altieri et al.,2024, 2015; Perfecto et al., 2019). They limit monoculture-driven pathogen amplification, reduce reliance on centralized inputs, and constrain the scale at which failures can propagate. Critically, agroecology provides direct defense against biological threats, both natural and engineered. Polyculture cropping systems disrupt the host density and spatial continuity that pathogens require for epidemic transmission, making it structurally more difficult for any single pathogen to cause systemic failure across a diversified landscape. Recent research demonstrates that polycultures promote complex root exudate chemistry that recruits plant-beneficial microbes, some of which enhance plants' innate immune system, providing a form of endogenous biological defense that monoculture systems lack (Altieri et al., 2024). From a CBS perspective, agroecology narrows both biological and digital attack surfaces: diverse cropping systems, localized production practices, and reduced dependence on uniform digital platforms make coordinated large-scale disruption more difficult (IPES-Food, 2016).

The empirical evidence for agroecological resilience is substantial. Diversified farming systems showed greater resistance and faster recovery than monocultures following both Hurricane Mitch and Hurricane Maria (Altieri et al.,2024, 2015; Perfecto et al., 2019). The mechanism is functional redundancy: communities with more species performing similar functions are buffered against the loss of any single species (Biggs et al., 2020). As Ulanowicz (2018) established, "biodiversity, functional redundancy, and system persistence are all entwined."

These parallels between agroecological resilience and cybersecurity resilience map onto specific defensive functions instead of being merely metaphorical. Applying cues from Saltzer et al. (1984) and Littlewood and Strignini (2004) across biology and into security, functional redundancy corresponds to heterogeneous, independent security pathways: farms operating diverse sensor networks, communication protocols, and software platforms, such that the compromise of any single system does not cascade across the entire operation. Polyculture diversity corresponds to a multi-vendor, multi-protocol digital infrastructure that limits correlated failure modes. Biological pest control through predator-prey dynamics and beneficial microbial communities corresponds to community-operated intrusion detection, in which distributed human and technical monitoring identifies anomalies through local knowledge rather than centralized algorithmic surveillance. Plant immune promotion through soil microbiome health aligns with security-by-design principles, in which systems are hardened at the foundational level rather than defended through layered external monitoring. In each case, the agroecological principle provides resilience through diversity, distribution, and endogenous defense. At the same time, BIOINT's unified surveillance architecture importantly enables faster detection but concentrates it in a single system whose compromise or deception could simultaneously blind the entire network. Security engineering research independently confirms that heterogeneous designs reduce the impact of successful attacks by preventing compromise from propagating uniformly (Saltzer et al., 1984; Littlewood and Strigini,

2004; Kott et al., 2015), as the July 2024 CrowdStrike incident, the technological equivalent of a pest epidemic in a monoculture, dramatically illustrated (Alsowaigh, 2025).

The IPES-Food (2016) report identified structural lock-ins preventing transition from industrial to diversified agriculture, each with a precise agricultural technology analogue. Path dependency maps onto proprietary platform dependency; power concentration maps onto the six-corporation consolidation of more than 60% of global seed sales and the digital platforms farmers depend on (IPES-Food, 2016; Sauvagerd et al., 2024). The centralized paradigm architecture adds a governance lock-in layer on top of the existing corporate one.

Stewart Brand's pace-layer framework acknowledges that nature is the slowest-changing layer of civilization (Brand, 2018). The implication: biosecurity strategies rooted in ecological integrity and cultural practices, the slow layers, are structurally more durable than solutions operating at the governance and commerce layers, where most CBS proposals concentrate. Agroecological diversity, soil microbiome health, and the plant immune functions they support operate at the pace of nature and culture. The FAO's Ten Elements of Agroecology, endorsed by 197 member states, provides a complementary framework emphasizing diversity, resilience, and responsible governance (FAO, 2018; Barrios et al., 2019). The centralized CBS paradigm identifies the right analytical framework but proposes fast-layer solutions to slow-layer problems.

5. Sovereignty-Centered Governance: From Bioaudits to Cooperative Assurance

Endy et al (2025)'s bioaudit proposal is among the report's most unique contributions. Modeled on financial auditing, it envisions independent third-party evaluations of biosafety and biosecurity practices, a credentialing process analogous to public accountant certification, and a Bioaudit Oversight Board modeled on the Public Company Accounting Oversight Board. The tiered verification framework, in which nations choose between unverified, self-verified, or multilaterally verified status, offers a pragmatic pathway for BWC modernization. The financial auditing analogy reveals structural risks that warrant further development. The history of financial auditing demonstrates that third-party verification within centralized hierarchies is susceptible to systemic capture: Enron, the 2008 financial crisis, and Wirecard all occurred under regimes of ostensibly independent audit oversight. A bioaudit board operating within the same institutional logic could benefit from mechanisms to mitigate analogous risks, particularly by clarifying who defines the standards against which audits are conducted.

Contemporary global bio-surveillance proposals describe large-scale biological data collection infrastructures incorporating metagenomic environmental sequencing, adaptive immune repertoire monitoring, and engineered living biosensors, often invoking anonymization and opt-in participation as governance safeguards that remain under-specified in technical detail; these are important functions via BIONT (Georgiou et al., 2014; Crits-Christoph et al., 2021; Mittelstadt and Floridi, 2016). This centralized CBS paradigm literature so far appears to not have deeply engaged with Indigenous data sovereignty frameworks, community consent mechanisms, or the political economy of biological surveillance data; data governance has considerable room to grow. This omission is particularly striking given that the world's largest technical professional organization has now codified Indigenous data governance as a technical standard: IEEE 2890-2025, the Recommended Practice for Provenance of Indigenous Peoples' Data, establishes parameters for recording data provenance related to Indigenous Peoples, their cultures, lands, and knowledge systems, and defines "data actors" to include non-human entities such as devices, applications, and AI systems (IEEE, 2025). The CARE Principles for Indigenous Data Governance, foregrounding collective benefit, authority to control, responsibility, and ethics, provide the normative foundation that IEEE 2890-2025 operationalizes (Carroll et al., 2023; IEEE, 2025). Leonelli's (2024) ethnographic research at Ghana's Crops Research Institute revealed that the push to digitize crop data as "global commons" can function as "a sophisticated form of bioprospecting and surveillance, whereby local knowledge of crops and their uses is harnessed and mined in ways that damage the very communities that produced it." Her subsequent work argues that dominant AI is underpinned by an anti-human philosophy of mastering nature, proposing instead "Environmental Intelligence" as the ability to live in and with nature (Leonelli, 2025), a vision aligned with the agroecological framework advanced here.

The alternative is cooperative assurance from below. Smallholder-led cooperatives could form associations to perform justice-accountable audits, retain shared access keys to models and datasets, and implement consent-by-design governance processes. Without such mechanisms, federated learning reproduces centralization in model control and monetization even as it decentralizes data storage: so long as smallholders lack meaningful governance over models and control over outputs, they remain data laborers rather than data owners (Zalik and Zalik, 2023). Manoj et al. (2025) demonstrate through AgriFLChain that blockchain-assisted decentralized identifiers and smart contracts can authenticate participants and govern model updates without reliance on a

central authority. The critical governance questions are: who decides which models are trained, who controls aggregation, and who sets the privacy parameters. In a sovereignty-centered framework, cooperative data governance boards, modeled on long-standing producer-led institutions such as the National Cooperative Dairy Herd Improvement Program (Wiggans et al., 2011), set research priorities through collective deliberation. Communities determine the differential privacy parameters, deciding how much privacy to trade for model accuracy.

Often, zero-knowledge proof proposals apply privacy-preserving verification to one narrow commercial checkpoint. Yet ZKPs, federated learning, and differential privacy belong to the same family of cryptographic approaches to decentralized trust, all solving structurally similar problems: deriving collective intelligence or verification from distributed data without requiring any party to surrender data to a central authority. Centralized CBS paradigms often glimpse this principle in one application but cannot follow through because generalizing it would require distributing governance authority to the communities whose data flows through the system, contradicting the centralized architecture on which the rest of the systems depend. Federated learning with community-governed differential privacy completes what the ZKP proposal begins, extending privacy-preserving verification from a single commercial transaction to the entire agricultural data ecosystem. The technical and institutional components for this alternative already exist. OpenTEAM and its farmOS platform provide interoperable, farmer-driven digital infrastructure through open APIs; L'Atelier Paysan demonstrates farmer-led technological sovereignty through open-source agricultural machinery (IPES-Food, 2016); and participatory guarantee systems in contexts from Mexico to India demonstrate that peer verification with social accountability can function as credible alternatives to centralized certification (Nelson et al., 2016; Ruder and Wittman, 2025).

6. Threat Model Considerations: Competing Risk Prioritizations and Discussions

Any framework for agricultural defense must specify what it defends against, at what cost, and what it sacrifices. The sovereignty-centered framework advanced here, and the centralized architecture proposed by the aforementioned dominant CBS paradigms, represent competing risk prioritizations rather than an ideological disagreement.

For ransomware and supply-chain attacks, decentralised or sovereignty-centred architectures offer structural advantages. Highly centralised systems create single points of failure, and in tightly coupled supply networks such failures can propagate as cascading disruptions across interdependent infrastructures (Rinaldi et al., 2001; Scheibe and Blackhurst, 2018; Ivanov et al., 2019). Decentralized systems operating on heterogeneous platforms with community-governed data infrastructure eliminate the high-value targets that ransomware operators preferentially seek. The centralized CBS architecture, which consolidates biosurveillance, certification, and coordination within unified federal systems, replicates the vulnerability pattern that enabled the JBS and cooperative software incidents at the governance level.

For novel engineered pathogen detection, the centralized framework holds an advantage in aggregation speed. Distributed sentinel systems may detect more slowly than a unified BIOINT system capable of cross-referencing metagenomic data across regions in real time. This paper does not claim that community governance eliminates the need for centralized analytical capacity in this threat class. However, three qualifications temper this concession. First, centralized systems may have failed to detect SARS-CoV-2 for approximately two months despite existing biosurveillance infrastructure (Pekar et al., 2021). Second, distributed systems are harder to spoof or systematically blind precisely because there is no single point of deception; an adversary must compromise multiple independent detection networks simultaneously rather than one unified system. Third, community-level monitoring creates human intelligence layers, farmers noticing anomalies in their crops, livestock, or soil that purely technical surveillance misses and that cannot be replicated by remote metagenomic sequencing. The agroecological foundation described in Section 4 adds a further layer: polyculture systems that disrupt pathogen transmission and promote plant immune function provide passive biological defense, reducing the probability that an engineered pathogen achieves epidemic spread in the first place (Altieri et al., 2024).

The sovereignty-centered framework addresses a third threat class that centralized CBS paradigms do not sufficiently appear to recognize: corporate data extraction and surveillance capitalism. BIOINT is a massive biological data-collection infrastructure that lacks engagement with the political economy of who controls that data or profits from it. Agricultural data is already subject to oligopolistic platformisation, in which four corporations control the majority of the digital platforms farmers depend on (IPES-Food, 2016; Sauvagerd et al., 2024). The FTC's 2025 suit against John Deere for unlawful repair cost inflation and for documenting $3 billion in annual farmer losses from tractor downtime illustrates how proprietary control functions as an ongoing

extraction mechanism (Rimmer, 2025). When farmers buy older equipment to avoid software on modern machinery, the cybersecurity implications are clear: proprietary systems actively prevent the distributed defense capacity that biosecurity requires (Wiens, 2018). A framework that treats corporate consolidation as external to biosecurity cannot address this threat class. A sovereignty-centered framework treats it as foundational.

Centralized CBS paradigms optimize for threat class 2 at the expense of threat classes 1 and 3. The sovereignty-centered framework optimizes differently, accepting a bounded trade-off in centralized detection speed in exchange for structural resilience against supply-chain attacks, systemic resistance to data extraction, and the endogenous biological defense that agroecological diversity provides against pathogens of any origin.

7. Conclusion: Toward Implementation

CBS needs a paradigm that treats centralization as a threat class, agroecology as defensive architecture, and sovereignty as a security requirement. This paper has argued that the strongest expression of the centralized paradigm, BIOINT, diagnoses the right threats but proposes an architecture that replicates the monoculture vulnerability identified in agriculture. The alternative advanced here, built on agroecological defense, sovereignty-preserving biosurveillance, and cooperative assurance from below, addresses threat classes that centralized frameworks structurally cannot see while engaging those they prioritize from a more resilient foundation.

Implementation can proceed through existing institutional infrastructure. In an initial phase, pilot deployments would build on operational cooperative platforms already in use: OpenTEAM and farmOS for interoperable farm data management, the National Cooperative Dairy Herd Improvement Program model for producer-led data governance, and participatory guarantee systems for peer-verified compliance (Nelson et al., 2016; Wiggans et al., 2011). A second phase would integrate decentralized federated learning with cooperative governance boards, using AgriFLChain-style blockchain-assisted authentication and community-set differential privacy parameters to enable collective threat detection without centralized data aggregation (Manoj et al., 2025). A third phase would establish a cross-cooperative federation, connecting regional sovereignty-preserving biosurveillance networks into broader detection systems that retain local governance authority over data and safety specifications. This phased pathway builds community governance capacity from below, with the two architectures designed to integrate bidirectionally rather than one subordinating the other.

This paper does not claim that technical safeguards can eliminate risk, nor does it claim that community governance is inherently immune to failure. Cooperative structures can fail through exclusion, elite capture, uneven capacity, or internal conflict. The sovereignty-centered framework does not eliminate the need for some centralized capacity for pathogen detection and genomic analysis, particularly for novel engineered threats. Agroecological transition is itself constrained by the very lock-ins this paper documents: path dependency, corporate consolidation, and policy environments that continue to privilege monoculture production (IPES-Food, 2016).

Stewart Brand's Pace Layer Framework notes that nature is the slowest-changing layer of civilization (Brand, 2018). Agricultural defense built on ecological integrity, soil microbiome health, community knowledge, and cooperative governance and slow layers provides a lasting and democratic foundation for any federal coordinating body, bioaudit regime, or AI-driven surveillance system. This paper argues that durable biosecurity emerges when the speed of detection is in relation with the depth of the systems, ecological and social, in which defense is rooted.

Acknowledgements

Special thanks go to the Spirit of Asilomar Next Generation Leaders Cohort and Indigenous Stewards (and their supporters). We acknowledge Dr. Jessica Snyder for proofreading and helpful comments.

Ethics Declaration

Ethical Clearance was not required.

AI Declaration

AI tools in Grammarly, Claude, ChatGPT, and Google Docs were used for literature searches and reviews, cross-referencing, formatting, spell-checking, and overall paper organization of pre-written text.

References

Aldhyani, T.H.H. and Alkahtani, H. (2023) 'Cyber security for detecting distributed denial of service attacks in Agriculture 4.0: Deep learning model', *Mathematics*, 11(1), p. 233. Available at: https://doi.org/10.3390/math11010233.

Alsowaigh, R.E. (2025) 'Crowdstrike causes global Microsoft outage: a case study', Journal of Information Security and Cybercrimes Research, 8(1), pp. 63–76. https://doi.org/10.26735/QHDD4798

Altieri, M.A., 2009. Agroecology, small farms, and food sovereignty. Monthly review, 61(3), pp.102-113.

Altieri, M.A., Nicholls, C.I., Henao, A. et al. (2015) 'Agroecology and the design of climate change-resilient farming systems', Agronomy for Sustainable Development, 35, pp. 869–890. doi:10.1007/s13593-015-0285-2.

Altieri, M.A., Nicholls, C.I., Dinelli, G. and Negri, L. (2024) 'Towards an agroecological approach to crop health: reducing pest incidence through synergies between plant diversity and soil microbial ecology', *npj Sustainable Agriculture*, 2, p. 6. Available at: https://doi.org/10.1038/s44264-024-00016-2.

Ashley, T., Gourisetti, S.N.G., Brown, N. and Bonebrake, C. (2022) 'Aggregate attack surface management for network discovery of operational technology', *Computers & Security*, 123, p. 102939. Available at: https://doi.org/10.1016/j.cose.2022.102939.

Barrios, E. *et al.* (2020) 'The 10 Elements of Agroecology: enabling transitions towards sustainable agriculture and food systems through visual narratives', *Ecosystems and People*, 16(1), pp. 230–247. doi: 10.1080/26395916.2020.1808705.

Biggs, C.R., Yeager, L.A., Bolser, D.G., Bonsell, C., Dichiera, A.M., Hou, Z., Keyser, S.R., Khursigara, A.J., Lu, K., Muth, A.F., Negrete, B. Jr. and Erisman, B.E. (2020) 'Does functional redundancy affect ecological stability and resilience? A review and meta-analysis', *Ecosphere*, 11(7), p. e03184. Available at: https://doi.org/10.1002/ecs2.3184.

Boyson, S. (2014) 'Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems', *Technovation*, 34(7), pp. 342–353. Available at: https://doi.org/10.1016/j.technovation.2014.02.001.

Brand, S. (2018) 'Pace Layering: How Complex Systems Learn and Keep Learning', *Journal of Design and Science* [Preprint]. doi:10.21428/7f2e5f08.

Carroll, S.R. et al. (2020) 'The CARE Principles for Indigenous Data Governance', *Data Science Journal*, 19, p. 43, pp. 1–12. Available at: https://doi.org/10.5334/dsj-2020-043.

Cartwright, A. and Cartwright, E. (2023) 'The economics of ransomware attacks on integrated supply chain networks', *Digital Threats*, 4(4), Article 56, pp. 1–14. Available at: https://doi.org/10.1145/3579647.

Crits-Christoph, A., Kantor, R.S., Olm, M.R., Whitney, O.N., Al-Shayeb, B., Lou, Y.C., Flamholz, A., Kennedy, L.C., Greenwald, H., Hinkle, A. and Hetzel, J., 2021. Genome sequencing of sewage detects regionally prevalent SARS-CoV-2 variants. MBio, 12(1), pp.10-1128. doi: 10.1128/mbio.02703-20

Dalrymple, D., Skalse, J., Bengio, Y., Russell, S., Tegmark, M., Seshia, S., Omohundro, S., Szegedy, C., Goldhaber, B., Ammann, N., Abate, A., Halpern, J., Barrett, C., Zhao, D., Zhi-Xuan, T., Wing, J. and Tenenbaum, J. (2024) 'Towards Guaranteed Safe AI: A Framework for Ensuring Robust and Reliable AI Systems', *arXiv preprint*, arXiv:2405.06624v2. Available at: https://arxiv.org/abs/2405.06624 (Accessed: 15 February 2026), https://doi.org/10.48550/arXiv.2405.06624.

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R.S. and Duncan, S.E. (2021) 'Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study', *Frontiers in Bioengineering and Biotechnology*, 9, 737927. doi:10.3389/fbioe.2021.737927.

Duncan, S.E., Reinhard, R., Williams, R.C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E. and Murch, R. (2019) 'Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System', *Frontiers in Bioengineering and Biotechnology*, 7, 63. doi:10.3389/fbioe.2019.00063.

Endy, D., Moront, S., Alexopoulos, V.A., Patel, R., Jain, R. and Bennett, B. (October 2025) *Biosecurity Really: A Strategy for Victory*. Stanford, CA: Hoover Institution, Bio-Strategies & Leadership Initiative.

FAO, 2018. The 10 Elements of Agroecology: Guiding the Transition to Sustainable Food and Agricultural Systems. Rome: Food and Agriculture Organization of the United Nations. Available at: https://openknowledge.fao.org/server/api/core/bitstreams/3d7778b3-8fba-4a32-8d13-f21dd5ef31cf/content (Accessed: 15 February 2026).

Gambino, A.J. (2023) 'Right to Repair: Whose Right is it Anyway?', *Tennessee Journal of Business Law*, 25(1), pp. 1–30. doi:10.70658/4486-1457.1650.

George, A.M. (2019) 'The National Security Implications of Cyberbiosecurity', *Frontiers in Bioengineering and Biotechnology*, 7, 51. doi:10.3389/fbioe.2019.00051.

Georgiou, G., Ippolito, G., Beausang, J. et al. (2014) 'The promise and challenge of high-throughput sequencing of the antibody repertoire', *Nature Biotechnology*, 32, pp. 158–168. doi:10.1038/nbt.2782.

Greenbaum, D. (2023) *Cyberbiosecurity : a new field to deal with emerging threats*. Cham, Switzerland : Springer. Available at: https://doi.org/10.1007/978-3-031-26034-6.

IEEE (2025) IEEE Recommended Practice for Provenance of Indigenous Peoples' Data. IEEE Std 2890-2025, pp. 1–25. Available at: https://ieeexplore.ieee.org/document/11302960 (Accessed: 15 February 2026).

IPES-Food (2016) *From Uniformity to Diversity: A Paradigm Shift from Industrial Agriculture to Diversified Agroecological Systems*. Brussels: International Panel of Experts on Sustainable Food Systems. Available at: http://www.ipes-food.org (Accessed: 15 February 2026).

Ivanov, D., Sokolov, B. and Dolgui, A. (2014) 'The Ripple effect in supply chains: trade-off 'efficiency-flexibility-resilience' in disruption management', *International Journal of Production Research*, 52(7), pp. 2154–2172. doi: 10.1080/00207543.2013.858836.

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. and Flores, W.N. (2025) *6.3 Community Biology: Advancing Responsible Biotech Innovation*. Houston, TX: Rice University. doi:10.25611/3QHJ-W351.

Jones, B.A., Grace, D., Kock, R., Alonso, S., Rushton, J., Said, M.Y., McKeever, D., Mutua, F., Young, J., McDermott, J. and Pfeiffer, D.U. (2013) 'Zoonosis emergence linked to agricultural intensification and environmental change', *Proceedings of the National Academy of Sciences*, 110(21), pp. 8399–8404. doi:10.1073/pnas.1208059110.

Knight, T. and Sureka, S. (2024) 'A New Paradigm for Threat Agnostic Biodetection: Biological Intelligence (BIOINT)', *Health Security*, 22(1), pp. 31–38. doi:10.1089/hs.2023.0072.

Kott, A., Alberts, D.S. and Wang, C. (2015) 'Will Cybersecurity Dictate the Outcome of Future Wars?', *Computer*, 48(12), pp. 98–101. doi:10.1109/MC.2015.359.

Leonelli, S. (2024) 'Globalizing plant knowledge beyond bioprospecting?', *History of Anthropology Review*, 48. Available at: https://histanthro.org/notes/globalizing-plant-knowledge/ (Accessed: 15 February 2026).

Leonelli, S. (2025) 'Rejoinder: Let Us Rescue Intelligence from Anti-Human AI', *Harvard Data Science Review*, 7(4). doi:10.1162/99608f92.4a868f98.

Littlewood, B. and Strigini, L. (2004) 'Redundancy and Diversity in Security', in Samarati, P., Ryan, P., Gollmann, D. and Molva, R. (eds.) *Computer Security – ESORICS 2004*. Lecture Notes in Computer Science, vol. 3193. Berlin: Springer, pp. 423–438. doi:10.1007/978-3-540-30108-0_26.

Manglicmot, M. (2022) 'Hackers are coming for our Thanksgiving turkeys and John Deere tractors. It's time to reevaluate America's food security', *Fortune*, 23 November. Available at: https://fortune.com/2022/11/23/hackers-thanksgiving-turkeys-john-deere-tractors-food-security-ransomware-cyberattacks-tech-mark-manglicmot/ (Accessed: 15 February 2026).

Manoj, T., Makkithaya, K. and Narendra, V. (2025) 'A Blockchain-Assisted Trusted Federated Learning for Smart Agriculture', *SN Computer Science*, 6, 221. doi:10.1007/s42979-025-03672-4.

Mittelstadt, B.D. and Floridi, L. (2016) 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts', *Science and Engineering Ethics*, 22(2), pp. 303–341. doi:10.1007/s11948-015-9652-2.

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, 39. doi:10.3389/fbioe.2018.00039.

National Academies of Sciences, Engineering, and Medicine (2018) Biodefense in the Age of Synthetic Biology. Washington, DC: The National Academies Press. https://doi.org/10.17226/24890

Nelson, E.M., Gómez Tovar, L., Gueguen, E., Humphries, S., Landman, K. and Schwentesius de Rindermann, R. (2016) 'Participatory guarantee systems and the re-imagining of Mexico's organic sector', *Agriculture and Human Values*, 33, pp. 373–388. doi: 10.1007/s10460-015-9615-x

Panigrahy, R. and Sharan, V. (2025) 'Limitations on safe, trusted, artificial general intelligence', *arXiv preprint*, arXiv:2509.21654. doi:10.48550/arXiv.2509.21654.

Pasca, E.M., Delinschi, D., Erdei, R., Baraian, I. and Matei, O.D. (2025) 'A Vulnerable-by-Design IoT Sensor Framework for Cybersecurity in Smart Agriculture', *Agriculture*, 15(12), 1253. doi:10.3390/agriculture15121253.

Peccoud, J., Gallegos, J.E., Murch, R., Buchholz, W.G. and Raman, S., 2018. Cyberbiosecurity: from naive trust to risk awareness. Trends in biotechnology, 36(1), pp.4-7.doi:10.1016/j.tibtech.2017.10.012

Pekar, J. et al. (2021) 'Timing the SARS-CoV-2 index case in Hubei province', *Science*, 372, pp. 412–417. doi:10.1126/science.abf8003.

Perfecto, I., Hajian-Forooshani, Z., Iverson, A. et al. (2019) 'Response of Coffee Farms to Hurricane Maria: Resistance and Resilience from an Extreme Climatic Event', *Scientific Reports*, 9, 15668. doi:10.1038/s41598-019-51416-1.

Perrow, C. (1999) *Normal Accidents: Living with High-Risk Technologies*. Updated edn. Princeton, NJ: Princeton University Press, ISBN: 9780691004129.

Powell, E., Akogo, D., Potter, L. and Palmer, X.L., 2021, October. Co-leadership and cross-pollination of university and DIY bio spaces: an exploration in consideration of Biocybersecurity. In Proceedings of the Future Technologies Conference (pp. 610-621). Cham: Springer International Publishing.

Puma, M.J., Bose, S., Chon, S.Y. and Cook, B.I., 2015. Assessing the evolving fragility of the global food system. Environmental Research Letters, 10(2), p.024007.

Rimmer, M., 2025. Tractor rage: Intellectual property, agriculture, competition policy, and the right to repair. *IIC-International Review of Intellectual Property and Competition Law*, 56(1), pp.115-152. doi: 10.1007/s40319-024-01538-5

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 21(6), pp.11-25. doi: 10.1109/37.969131

Ruder, S.L. and Wittman, H., 2025. Agricultural data governance from the ground up: Exploring data justice with agri-food movements. *Big Data and Society*, 12(1), p.20539517251330182. doi:10.1177/20539517251330182

Saltzer, J.H., Reed, D.P. and Clark, D.D., 1984. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, 2(4), pp.277-288. doi:10.1145/357401.357402

Sauvagerd, M., Mayer, M. and Hartmann, M., 2024. Digital platforms in the agricultural sector: Dynamics of oligopolistic platformisation. *Big Data and Society*, 11(4), p.20539517241306365. doi:10.1177/20539517241306365

Scheibe, K.P. and Blackhurst, J., 2018. Supply chain disruption propagation: a systemic risk and normal accident theory perspective. International journal of production research, 56(1-2), pp.43-59. doi:10.1080/00207543.2017.1355123

Sick Codes, 2021. DEF CON 29: The agricultural data arms race: Exploiting a tractor load of vulns [online video]. YouTube. Available at: https://youtu.be/zpouLO-GXLo

Sick Codes, 2022. DEF CON 30: Hacking the farm: Breaking badly into agricultural devices [online video]. YouTube, 18 August. Available at: https://youtu.be/z2_TLz9TpwY

Stephen, S., Alexander, K., Potter, L. and Palmer, X.L., 2023. Implications of cyberbiosecurity in advanced agriculture. doi:10.34190/iccws.18.1.995

Tegmark, M. and Omohundro, S., 2023. Provably safe systems: the only path to controllable AGI. *arXiv preprint arXiv:2309.01933*.

Tomašev, N., Franklin, M., Jacobs, J., Krier, S. and Osindero, S., 2025. Distributional AGI safety. *arXiv preprint arXiv:2512.16856*.

Ulanowicz, R.E., 2018. Biodiversity, functional redundancy and system stability: subtle connections. *Journal of The Royal Society Interface*, 15(147), p.20180367. doi:10.1098/rsif.2018.0367

Wiens, K., 2018. We can't let John Deere destroy the very idea of ownership. Wired, 7 February. Available at: https://www.wired.com/story/john-deere-farmers-right-to-repair/

Wiggans, G.R., VanRaden, P.M. and Cooper, T.A., 2011. The genomic evaluation system in the United States: Past, present, future. *Journal of Dairy Science*, 94(6), pp.3202-3211. doi: 10.3168/jds.2010-3866

Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A.G., Russell, C. and Duncan, E., 2021. A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences*, 11(16), p.7518. doi: /10.3390/app11167518

Zalik, K.R. and Zalik, M., 2023. A review of federated learning in agriculture. *Sensors*, 23(23), p.9566. doi: 10.3390/s23239566