Cyber-foci on Biofabrication: Conceptually Exploring Cybersecurity Risks and Mitigation Strategies in 3D Bioprinting Systems

Oludolamu Onimole[1], Dodzi Koku Hattoh[2,3], Abigail Oppong[4], Jude Osamor[5], Danny "Danhammer" Hetzel[6,7], Lucas Potter[8] and Xavier-Lewis Palmer[7,8]

[1]Independent Researcher, Glasgow, UK
[2]Ethics Lab, Philosophy & Classics, University of Ghana
[3]Bonn Sustainable AI Lab, UniBonn, Germany
[4]Independent Researcher, Accra, Ghana
[5]Department of Cybersecurity & Networks, Glasgow Caledonian University, UK
[6]Husaria Security, WI, USA
[7]Biohacking Village, USA
[8]BiosView Labs, Dayton, OH, USA

oludolamuonimole@gmail.com

Abstract: 3D bioprinting converges digital design, embedded firmware, and biological materials, creating a complex bio-cyber-physical ecosystem where digital compromise threatens fabrication reliability, data integrity, and potential biological performance. This paper presents a critical narrative review, informed by a structured multidisciplinary literature search, synthesizing evidence from bioprinting, additive manufacturing, industrial control systems, and cyberbiosecurity to identify critical attack surfaces and mitigation strategies. The review distinguishes between risks demonstrated directly in bioprinting, evidence transferred from adjacent cyber-physical domains, and theoretically plausible scenarios. Principal threats identified include firmware compromise, malicious machine-instruction manipulation, network vulnerabilities, and supply-chain attacks. While firmware and additive-manufacturing instruction attacks are well-documented, direct evidence linking digital compromise to clinically significant biological harm remains limited; thus, the provided threat mappings and attack pathways function as conceptual tools rather than validated quantitative risk models. To address these vulnerabilities, a layered defence approach is proposed, integrating hardware roots of trust, secure boot, firmware and file integrity, network segmentation, and robust biological quality assurance. Although artificial intelligence and machine learning offer promise for advanced telemetry analysis and anomaly detection, their deployment is currently constrained by model opacity, limited domain-specific datasets, and vulnerability to adversarial manipulation. These technical measures must be supported by human-centred controls, including role-specific training and multidisciplinary incident response. Ultimately, cybersecurity must be embedded throughout the full bioprinting lifecycle, with future research prioritizing reproducible attack experiments, shared benchmark datasets, evidence-qualified risk metrics, and the validation of security controls on representative laboratory and clinical platforms.

Keywords: 3D bioprinting, Cybersecurity, Cyberbiosecurity, Artificial intelligence, G-code injection, Firmware security, Industrial control systems, Biomanufacturing, Supply chain security

1. Introduction

Three-dimensional (3D) bioprinting has revolutionized the fabrication of complex biological constructs for tissue engineering, disease modelling, regenerative medicine, and personalized healthcare by enabling the precise deposition of cells, biomaterials, and bioactive components. However, the increasing automation and data-intensity of these systems, exemplified by recent advancements in self-driving and computationally integrated bioprinting (Liu et al., 2026), have heightened reliance on digital design files, slicing software, embedded controllers, sensors, firmware, and networked services. Consequently, these systems function as bio-cyber-physical entities where digital instructions directly dictate physical fabrication and biological outcomes (Yampolskiy et al., 2018; Ahsan et al., 2024). This convergence introduces significant vulnerabilities; unauthorized modification of firmware, machine instructions, sensor data, or design files could compromise deposition fidelity, construct geometry, and cell viability, or lead to the exposure of patient-related information, proprietary formulations, and experimental designs.

These vulnerabilities fall within the burgeoning field of cyberbiosecurity, which addresses security risks at the interface of digital infrastructure and biological systems (Murch et al., 2018; Naik et al., 2026). Given that cyberbiosecurity should be delimited by consequence rather than discipline, the field is best defined by systems where cyber disruption produces a measurable biological consequence (Pope, 2026). This framework is particularly salient for bioprinting, as it allows for the differentiation of conventional cybersecurity concerns, such as data theft, from incidents that threaten cell viability, construct integrity, or other tangible biological outcomes.Nevertheless, the evidentiary base for these risks remains nuanced and uneven. While firmware

compromise has been demonstrated directly within bioprinting contexts (Ahsan et al., 2025), other threats such as malicious machine-instruction modification, side-channel leakage, and supply-chain attacks are predominantly documented in conventional additive manufacturing. Furthermore, risks transferred from industrial control systems, connected healthcare, and IoT environments remain theoretically plausible rather than empirically established for bioprinting, necessitating caution against overstating the field's maturity.

The introduction of artificial intelligence (AI) and machine learning (ML) further complicates this risk landscape. While these tools significantly enhance design optimization, printability assessment, and process monitoring (Malekpour and Chen, 2022; Piotrowska et al., 2025), they introduce vulnerabilities related to model opacity, limited training data, false alarms, and susceptibility to adversarial manipulation. To navigate these complexities, this paper presents a critical narrative review, informed by a structured multidisciplinary literature search, to synthesize the principal cybersecurity threats to 3D bioprinting and evaluate layered technical and organizational controls. By distinguishing between direct bioprinter evidence and adjacent findings, this study offers an evidence-qualified framework for understanding cyber risks and defence priorities.

2. Review Methodology

This study adopts a critical narrative review informed by a structured multidisciplinary literature search. This design was selected because cybersecurity research specific to 3D bioprinting remains limited and is distributed across several related fields, including biofabrication, additive manufacturing, cyber-physical systems, embedded-device security, industrial control systems, artificial intelligence, and cyberbiosecurity. The review therefore aims to integrate heterogeneous evidence and assess its relevance to bioprinting rather than claim exhaustive retrieval or statistical synthesis. Literature published between 2015 and 2026 was identified through PubMed, Scopus, IEEE Xplore, and Google Scholar. Search concepts combined terms relating to 3D bioprinting and biofabrication with cybersecurity, cyberbiosecurity, additive-manufacturing security, firmware attacks, malicious G-code, network intrusion, side-channel leakage, supply-chain compromise, anomaly detection, machine learning, and zero-trust architectures. Reference lists of relevant reviews and foundational studies were also examined to identify additional sources.

Peer-reviewed journal articles and conference papers were prioritized. Selected standards, government publications, technical reports, and industry sources were included where they provided relevant operational, regulatory, workforce, or security context. Sources were considered eligible when they addressed cybersecurity vulnerabilities in bioprinting or additive manufacturing; security of connected biomedical or cyber-physical systems; firmware, software, network, hardware, side-channel, sensor, or supply-chain threats applicable to bioprinting; AI-supported defensive mechanisms; or governance and workforce issues relevant to secure biofabrication. Publications concerned only with bioprinting performance were used to support claims about process sensitivity and biological consequences, but not as evidence that cyberattacks had occurred.

The literature was synthesized thematically according to system architecture, attack surface, potential operational or biological consequence, mitigation mechanism, implementation limitation, and evidentiary maturity. To avoid overstating the available evidence, findings were classified as: direct evidence from bioprinting systems; adjacent evidence from conventional additive manufacturing; transferred evidence from related cyber-physical, IoT, medical-device, or industrial-control environments; or theoretically plausible bioprinting-specific scenarios. Within these categories, the review further distinguished ordinary cybersecurity consequences from cyber disruptions capable of producing measurable biological consequences, consistent with the consequence-focused framework proposed by Pope (2026).

The classification also reflects a consequence-based interpretation of cyberbiosecurity. Following Pope (2026), a security event was treated as specifically cyberbiosecurity-relevant where cyber disruption could plausibly produce a measurable biological consequence. Events limited to confidentiality, availability, financial loss, or equipment disruption were retained as cybersecurity concerns relevant to bioprinting but were not treated as evidence of biological consequence unless an explicit cyber-to-biological pathway could be identified.

3. Bioprinting Technologies, Threats, and Consequences

3.1 Modalities and System Architecture

The principal 3D bioprinting modalities are extrusion-based, inkjet-based, and laser-assisted bioprinting. Extrusion systems deposit continuous filaments of relatively viscous bioink using pneumatic, piston, or screw-driven mechanisms. Their performance depends on parameters such as pressure, temperature, nozzle motion, material viscosity, and deposition speed (Betancourt and Chen, 2022; Malekpour and Chen, 2022). Inkjet

systems use thermal or piezoelectric actuation to deposit discrete droplets and require precise control of droplet volume, timing, nozzle operation, and positioning (Ng and Shkolnikov, 2024; Gupta et al., 2025). Laser-assisted systems use focused laser energy to transfer bioink from a donor substrate and depend on accurate control of pulse energy, timing, alignment, and positioning (Dou et al., 2021; Shakil Arman et al., 2023).

Despite their mechanical differences, these platforms increasingly share common digital components, including design and slicing software, embedded controllers, firmware, graphical interfaces, sensors, network connections, remote-maintenance functions, and cloud services. Their cybersecurity exposure therefore depends not only on the printing modality but also on the complete system architecture. A stand-alone laboratory printer may have a smaller remotely accessible attack surface than a platform supporting cloud-based job submission and over-the-air updates, although isolation does not eliminate risks from removable media, malicious insiders, compromised components, or unauthorized local access.

3.2 Principal Attack Vectors

Table 1 maps Evidence-qualified cybersecurity risks in 3D bioprinting. Firmware compromise is one of the most directly supported risks. Firmware controls low-level functions such as movement, heating, extrusion, sensing, and safety enforcement. Ahsan et al. (2025) demonstrated firmware attacks in a 3D bioprinting context, showing that malicious embedded control logic can affect printer operation and physical output. The precise consequences remain platform-specific: altered firmware could plausibly modify extrusion pressure in an extrusion system, droplet timing in an inkjet system, or laser parameters in a laser-assisted system.

Digital designs and machine instructions form a second important attack surface. Studies of conventional additive manufacturing show that malicious changes to G-code or toolpaths can interrupt production, alter geometry, conceal defects, or otherwise modify physical outcomes (Yampolskiy et al., 2018; Pearce et al., 2022; Rossel et al., 2025). Comparable manipulation in bioprinting could affect deposition paths, layer structure, flow rate, droplet placement, or energy delivery. Detecting such interference may be complicated by the substantial variability and limited standardization of bioprinting processes (Grijalva Garces et al., 2024). Printing outcomes depend on interactions among bioink rheology and composition, equipment configuration, process parameters, and the biological material being printed (Schwab et al., 2020). These factors produce inherent deviations in filament dimensions, material deposition, shape fidelity, cell viability, and construct morphology. Bioprinting can exhibit substantial process variability originating from interactions amongst bioink properties, printing conditions, equipment, and other operator dependent factors, with the reproducibility remaining a commonly recognized challenge across laboratories (Grijalva Garces et al., 2024). This elevated baseline of process variation could obscure malicious interference, as subtle cyber-manipulations are more easily misclassified as routine process noise or experimental failure. Consequently, the detection of deliberate interference amidst such significant background variability remains a substantial challenge (Ahsan et al., 2024). Direct evidence linking digital-design manipulation to measurable biological harm, however, remains limited.

Network connectivity introduces further risks. Remote diagnostics, job submission, cloud analytics, web interfaces, and application programming interfaces may expose systems to weak authentication, default credentials, insecure communications, outdated software, or excessive privileges. These weaknesses are well established in IoT and connected-healthcare environments (Sahoo et al., 2020), but their prevalence across commercial bioprinters has not been systematically assessed. Supply-chain compromise may arise through software dependencies, firmware, replacement components, control boards, sensors, third-party services, or outsourced design and production processes. Additive-manufacturing research identifies supply-chain integrity as a significant concern because compromise may occur before a file or component reaches the operating laboratory (Yampolskiy et al., 2018; Gupta et al., 2020). Specific scenarios involving malicious bioprinter cartridges or optical modules remain largely theoretical unless supported by direct evidence.

Side-channel attacks exploit physical emissions rather than conventional network access. Acoustic and magnetic signals have been used to infer aspects of conventional 3D-printer operation and reconstruct information about printed designs (Song et al., 2016). Figure 1 illustrates a conceptual progression from reconnaissance and initial access through persistence, lateral movement, command and control, and manipulation of firmware or machine instructions. It synthesizes evidence from bioprinter firmware research, conventional additive-manufacturing security, and broader cyber-physical threat models and should not be interpreted as a documented end-to-end attack against a clinical bioprinting system (Yampolskiy et al., 2018; Ahsan et al., 2025; Rossel et al., 2025).

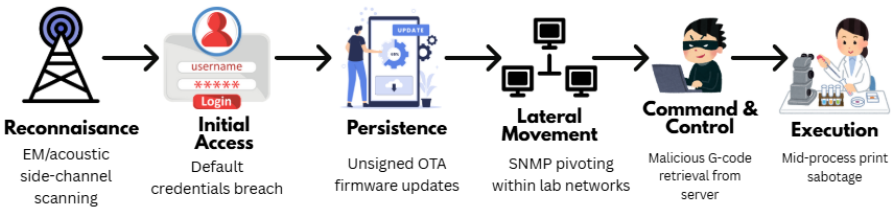

Figure 1: Conceptual attack kill-chain flow for a networked 3D bioprinting system

Sensor and telemetry manipulation represents another potentially transferable risk. Bioprinters often employ sensors for pressure, temperature, flow, positioning, imaging, and environmental monitoring to facilitate closed-loop control. Consequently, falsified telemetry could theoretically conceal abnormal operation or induce automated systems to make inappropriate, potentially deleterious adjustments. While measurement-manipulation and deception attacks are well-characterized in the broader industrial cyber-physical systems literature (Zhang et al., 2021), their applicability to and specific biological consequences for bioprinting platforms remain under-investigated.

Table 1: Some Cybersecurity risks in 3D bioprinting

Threat	Relevant layer	Potential consequence	Biological-consequence pathway	Evidence status
Firmware manipulation	Embedded control	Altered movement, pressure, temperature, sensing, or safety logic	May change conditions affecting cell viability or construct integrity	Direct bioprinter evidence
Malicious machine instructions	Design, slicing, G-code, or toolpath	Altered geometry, interruption, or concealed defects	May alter deposition fidelity, material distribution, or biological performance	Adjacent experimental evidence
Network compromise	Remote services and infrastructure	Unauthorized access, disruption, or data theft	Biological consequence only where compromise affects fabrication or process control	Transferred evidence
Supply-chain compromise	Hardware, software, firmware, and services	Persistent vulnerabilities or modified components	May affect trusted control of biologically sensitive processes	Adjacent evidence
Side-channel leakage	Physical emissions	Disclosure of design or operational information	Usually a confidentiality risk unless linked to subsequent biological manipulation	Adjacent experimental evidence
Sensor manipulation	Telemetry and closed-loop control	Concealed deviation or inappropriate automated response	May alter biological process conditions through corrupted feedback	Transferred evidence

3.3 Operational and Biological Consequences

Security failures may produce operational, informational, physical, or biological consequences. This distinction is important because not every cyber incident affecting a bioprinter necessarily constitutes a cyberbiosecurity event. Under a consequence-first approach, compromise becomes specifically cyberbiosecurity-relevant when the digital disruption produces, or creates a demonstrable pathway toward, a measurable biological consequence (Pope, 2026). Denial-of-service attacks, ransomware, or design-file theft may therefore remain conventional cybersecurity incidents unless they also affect living materials, biological process conditions, construct integrity, or biological function. Biological consequences require greater caution. The cited bioprinting literature establishes that extrusion pressure, shear stress, droplet behaviour, laser energy, and deposition accuracy can influence printability, cell viability, and construct quality (Dou et al., 2021; Betancourt and Chen, 2022; Malekpour and Chen, 2022; Shakil Arman et al., 2023; Ng and Shkolnikov, 2024; Gupta et al., 2025). It is therefore plausible that malicious alteration of these parameters could affect biological performance. Process sensitivity, however, is not equivalent to proof of cyber-induced harm.

Matai et al. (2020) identify controlled architecture, heterogeneous cell distribution, and geometric precision as important advantages of 3D bioprinting. Cybersecurity compromise could erode these benefits by reducing confidence in the authenticity of design files, consistency of machine behaviour, and integrity of process data. The strongest current evidence concerns technical compromise and altered physical output; clinically significant

biological consequences remain largely theoretical and require experiments linking digital manipulation to machine deviation, construct-level change, and measurable biological effect.The risks summarized in Table 1 should therefore be interpreted as an evidence-qualified threat map rather than a ranking of attack probability. Their relevance depends on the printer's modality, firmware, connectivity, operating environment, and quality-control procedures.

4. Comparison of Bioprinting Modalities and Cyberbiosecurity Perspectives

Protecting 3D bioprinting requires defence in depth across hardware, firmware, software, machine instructions, networks, telemetry, and biological quality assurance. No single control can secure a system in which digital commands directly influence physical fabrication and living materials. The controls proposed here are drawn from embedded-system, industrial-control, additive-manufacturing, and general cybersecurity practice; most remain insufficiently validated in operational bioprinting environments.

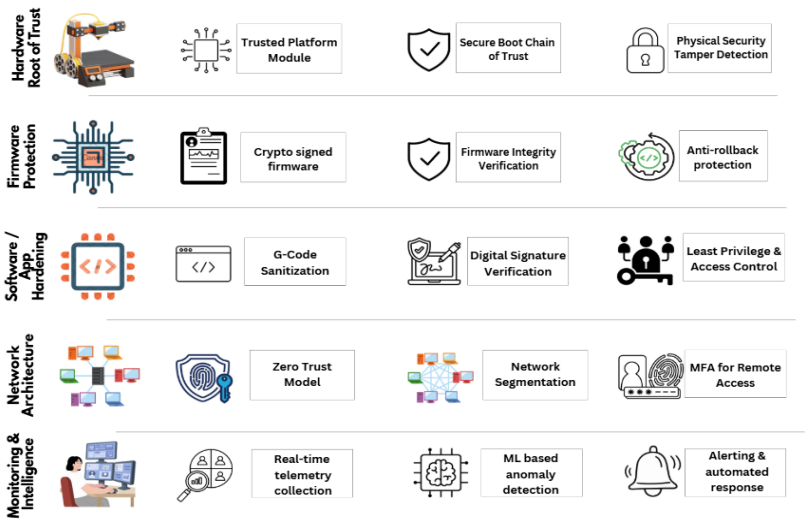

Figure 2: Conceptual layered defence architecture for 3D bioprinting systems

As shown in Figure 2, the proposed architecture progresses from hardware trust and firmware integrity through file and machine-instruction assurance, network and identity controls, telemetry monitoring, and biological quality assurance. The layers are intended to provide overlapping protection so that failure of one control does not automatically permit compromise of the fabrication process.

4.1 Foundational Technical Controls

Hardware-backed trust can strengthen device identity, protect cryptographic material, and support secure boot. Physical access to control boards, debug interfaces, removable-media ports, and maintenance connectors should likewise be restricted. Although such protections may be difficult to retrofit into proprietary or legacy platforms, they reduce dependence on software-only controls and limit opportunities for unauthorized modification at the device level.

Firmware should be treated as a critical security boundary. Secure boot, cryptographic signing, authenticated updates, rollback protection, and persistent version logging can reduce the likelihood of unauthorized low-level code execution. These controls are especially relevant because firmware-level attacks have already been demonstrated in a bioprinting context (Ahsan et al., 2025). Their effectiveness, however, depends on secure key management, vendor support, transparent update procedures, and reliable mechanisms for recovery from failed or malicious updates.

Digital design files and machine instructions should be protected throughout the design-to-print workflow. Authenticated repositories, version control, cryptographic hashes, digital signatures, access logging, and pre-execution integrity checks can help ensure that the file released for fabrication is the same file that was reviewed and approved. Machine instructions should also be validated for unauthorized commands, anomalous movements, unsafe pauses, and parameter values outside approved operating ranges. This distinction is important because a file may be syntactically valid while still encoding parameters capable of producing biologically damaging outcomes.

Network-connected bioprinters should be segmented from general institutional networks, unnecessary services should be disabled, and remote access should be tightly controlled. Administrative, vendor, and maintenance access should use strong authentication, device-specific credentials, and least-privilege authorization. Authentication alone, however, should not confer permission to perform safety-critical operations. High-impact functions, including firmware installation, calibration changes, modification of safety or process limits, and execution of externally supplied print jobs, should require explicit function-level authorization and, where consequences may be substantial, secondary approval or equivalent procedural verification. Multi-factor authentication is particularly appropriate for remote maintenance, firmware management, cloud administration, and other privileged functions. These controls should also be aligned with laboratory workflows so that security requirements remain operationally usable and do not incentivize unsafe workarounds.

4.2 AI-supported Monitoring

Bioprinters may generate telemetry relating to motor current, movement, temperature, pressure, flow, droplet actuation, laser operation, and environmental conditions. Rule-based limits can detect known unsafe states, while machine-learning models may identify multivariate or temporal deviations that are less visible through fixed thresholds. This is relevant because machine learning is already used in bioprinting for printability assessment, process modelling, and outcome prediction (Malekpour and Chen, 2022; Piotrowska et al., 2025). AI-supported anomaly detection could compare current telemetry with validated print profiles, flag unusual machine behaviour, or identify discrepancies between commanded and observed operation. It may also support pre-print screening by detecting unexpected changes in design files, toolpaths, or parameter combinations.

These systems remain experimental. Ordinary process variation, changes in bioink properties, calibration drift, nozzle condition, and environmental factors may generate false alarms if anomaly-detection thresholds are insufficiently calibrated (Ahsan et al., 2024). Models trained on one printer or material may not transfer reliably to another (Shin et al., 2022). Telemetry itself may also be spoofed, training data poisoned, or models manipulated to evade detection.For safety or biologically significant process variables, monitoring derived from an independent trust domain may provide stronger assurance than telemetry generated by the same controller responsible for process execution. AI outputs should therefore complement rather than replace deterministic safety limits, file-integrity controls, protected logs, and expert review. Predictive risk scores should be treated as decision-support tools rather than estimates of attack probability. At present, the field lacks sufficiently large and representative datasets to support precise quantitative claims (Sun et al., 2023). Explainability is also important: operators should be able to determine whether an alert arose from a network event, integrity failure, unusual command, or process deviation.

4.3 Integrated Assurance and Incident Response

Cybersecurity monitoring should be connected to manufacturing and biological quality assurance. Cybersecurity evidence may reveal unauthorized modification without establishing whether the printed construct was affected, while biological or manufacturing quality assessment may identify an abnormal output without establishing a cyber cause. Effective assurance therefore requires correlation of digital-integrity evidence, machine and process telemetry, in-process inspection, and post-print quality observations (Brandman et al., 2020; Raeker-Jordan et al., 2024; Sergis et al., 2025). This integration is particularly important in bioprinting because changes to process parameters can affect both construct fidelity and cellular performance (Wang, Cui and Maniruzzaman, 2023). Reliable time synchronization across controllers, workstations, network services, and monitoring systems should provide a common temporal reference for reconstructing event sequences and correlating cyber events with process and quality anomalies (Lévesque and Tipper, 2016). Changes to process-critical parameters should therefore be retained as part of the security record so that fabrication or biological anomalies can be traced against preceding digital modifications and other relevant system events (Brandman et al., 2020; Raeker-Jordan et al., 2024).

Where compromise is suspected, affected prints should be quarantined pending assessment. Incident-response procedures should cover device isolation, preservation of logs, firmware and software verification, credential reset, calibration checks, biological evaluation, and validated recovery. Responsibilities should be shared across cybersecurity, engineering, laboratory quality, biosafety, and clinical personnel where applicable. Defense layers, principal controls, and main limitations are listed below in Table 2.

Table 2: Layered controls and implementation limitations

Defense layer	Principal controls	Main limitation
Hardware and firmware	Hardware trust, secure boot, signed updates, rollback protection	Vendor dependence and limited retrofit options
Files and instructions	Provenance, signatures, version control, parameter validation	Modality-specific safety limits and workflow complexity
Network and access	Segmentation, least privilege, multifactor authentication, secure remote access	Administrative burden if poorly designed
Monitoring	Protected telemetry, fixed thresholds, command–observation comparison, anomaly detection	False positives, sensor compromise, limited datasets
Biological assurance	In-process inspection, viability checks, quarantine, incident response	Limited evidence linking cyber alerts to biological harm

A practical baseline should prioritize asset inventory, elimination of default credentials, authenticated firmware updates, controlled access to files, network segmentation, pre-print validation, protected logging, and documented recovery procedures. More advanced controls, including hardware-backed attestation and AI-supported monitoring, should be adopted according to risk, platform capability, and available evidence.

5. Human, Organizational, and Governance Controls

Technical safeguards are effective only when personnel understand and follow the procedures that support them. In 3D bioprinting, responsibility is distributed across biomedical engineers, laboratory technicians, software developers, cybersecurity staff, quality managers, clinicians, and vendors. Human-centred security should therefore form part of the wider defence architecture rather than being treated as a separate compliance activity.

Credential misuse, phishing, social engineering, and operational error remain important contributors to cybersecurity incidents across sectors (Verizon, 2024). Research also indicates that security knowledge, attitudes, and behaviour influence organizational outcomes (Parsons et al., 2014; Hadlington, 2017). Although these findings are not specific to bioprinting, they are relevant to laboratories that rely on shared workstations, remote services, digital design files, removable media, and third-party maintenance access.

Training should be role-specific. Operators need to verify file provenance, recognize unexpected parameter changes, use secure authentication, handle removable media safely, interpret alerts, preserve logs, and quarantine potentially affected constructs. Cybersecurity specialists must understand that process anomalies may have biological significance, while laboratory and quality personnel require clear escalation procedures when digital compromise is suspected. Responsibility for firmware analysis, biological assessment, incident reporting, and recovery should be assigned in advance.

AI-supported learning and simulation may help address differences in expertise across multidisciplinary teams. Adaptive systems can tailor learning content and guidance to individual cybersecurity training needs (Kallonas, Piki and Stavrou, 2024), while cyber ranges and security testbeds can provide realistic, simulated, emulated, or hybrid environments in which personnel can rehearse cyber incidents without requiring equivalent exercises on live operational systems (Yamin, Katt and Gkioulos, 2020; Chouliaras et al., 2021). Relevant exercises may include malicious file submission, firmware compromise, credential theft, ransomware, sensor manipulation, and supply-chain anomalies.

These tools should supplement rather than replace expert-led training. AI-based educational systems may collect sensitive learner data, reinforce bias, or provide decontextualized guidance. Their use, therefore, requires transparency, privacy protections, human review, and accessible alternatives for institutions with limited resources.

Governance should also define vulnerability reporting, vendor responsibilities, update approval, incident escalation, evidence preservation, and the conditions under which a printer or construct may return to use.

Effective cyberbiosecurity depends on coordinated technical, biological, and organizational decision-making rather than isolated awareness training.

6. Discussion, Limitations, and Research Priorities

Drawing upon the organizational controls identified in the previous section, it is necessary to calibrate these strategies against the current state of empirical knowledge. Cybersecurity risks in 3D bioprinting are credible but unevenly evidenced. The strongest direct evidence concerns firmware compromise in a bioprinting context (Ahsan et al., 2025), whereas malicious machine instructions, supply-chain attacks, and side-channel leakage are supported mainly by conventional additive-manufacturing research (Song et al., 2016; Yampolskiy et al., 2018; Gupta et al., 2020; Pearce et al., 2022; Rossel et al., 2025). Network and sensor risks are largely transferred from Internet of Things, connected-healthcare, and industrial-control environments (Sahoo et al., 2020). Biological consequences remain the least mature component of the evidence base. Crucially, this evidentiary heterogeneity complicates the definition of cyberbiosecurity boundaries. Being informed by Pope (2026), the discipline should be delimited not by categorical association with biology, but by the presence of a measurable biological consequence. Applied to the bioprinting context, this consequence-first paradigm mandates that cyber events such as data exfiltration, ransomware, or network compromise be distinguished from true cyberbiosecurity incidents, which necessitate a demonstrable pathway to altered cell viability, compromised construct integrity, or other tangible biological disruption.

This conceptual rigor is essential to prevent taxonomic over-extension, ensuring that security resources are directed toward events with verified biological impact. Mitigation strategies exhibit a similar unevenness. While foundational controls such as secure boot, signed firmware, network segmentation, least-privilege access, and file-integrity verification are mature in adjacent fields, their efficacy in complex bioprinting environments requires further validation. Conversely, AI-supported monitoring remains in a nascent state, hindered by limited domain-specific training data, the inherent variability of bioinks and equipment, false alarms, and susceptibility to adversarial manipulation. Consequently, these predictive tools should currently serve as an adjunct to, rather than a replacement for, deterministic rule-based process controls and human oversight. Looking forward, the research agenda must prioritize four imperatives: the conduct of controlled attack studies across representative bioprinting modalities; the establishment of shared telemetry repositories and benchmark datasets; the development of explainable AI (XAI) security tools; and the standardization of risk terminology to distinguish between attack feasibility, operational consequence, and biological harm. Although this review is constrained by its reliance on a critical narrative design and transferred evidence, these research priorities offer a pathway toward evidence-qualified frameworks. Integrating these security measures into regulatory sandboxes and laboratory governance as advocated by broader cyberbiosecurity scholarship (Murch et al., 2018; Reed and Dunaway, 2019; Potter and Palmer, 2023; Elgabry and Johnson, 2024; acpi et al., 2024) can protect the translational promise of 3D bioprinting infrastructure.

7. Conclusion

3D bioprinting establishes a critical bio-cyber-physical ecosystem where digital compromise threatens fabrication reliability, data security, process integrity, and biological performance. Evidence remains heterogeneous: while firmware vulnerabilities are directly demonstrable, many other threats including malicious machine-instruction manipulation, side-channel leakage, and supply-chain attacks are largely extrapolated from adjacent additive manufacturing or cyber-physical domains, and direct evidence linking these to clinically significant biological harm remains limited. A proportionate security strategy should therefore prioritize foundational, mature controls, such as firmware authentication, secure boot, robust network segmentation, and rigorous incident response, integrated seamlessly with biological quality assurance. While artificial intelligence and machine learning offer potential for enhanced anomaly detection and risk prioritization, their deployment must remain bounded by deterministic safety limits, transparent decision-making, and expert human oversight. Given the conceptual nature of this current threat framework, future research should prioritize reproducible attack studies on representative bioprinting platforms, the development of standardized datasets, and validated security metrics. Embedding comprehensive cybersecurity throughout the design-to-fabrication lifecycle is essential to protecting the safety, resilience, and long-term translational promise of 3D bioprinting infrastructure.

Ethics Declaration: This review did not involve human participants, animals, identifiable personal data, or clinical interventions. Ethical approval and informed consent were therefore not required.

AI Declaration: AI-assisted functions available through Grammarly and Google Docs were used for spelling, grammar, and organizational support. The authors reviewed suggested changes and retained full responsibility for the manuscript's content, interpretation, citations, and conclusions.

References

Ahsan, M., Najarro-Blancas, B., Ebode, J.T., Lewinski, N. and Ahmed, I. (2025) '3D bioprinter firmware attacks: Categorization, implementation, and impacts', *Proceedings of the 2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 99–110. doi: 10.1109/HOST64725.2025.11050047.

Ahsan, M., Pak, E., Jackson, K., Rais, M.H., Najarro-Blancas, B., Lewinski, N. and Ahmed, I. (2024) 'BioSaFe: Bioprinting security framework for detecting sabotage attacks on printability and cell viability', *Proceedings of the 2024 Annual Computer Security Applications Conference (ACSAC)*, pp. 271–287. doi: 10.1109/ACSAC63791.2024.00036.

Arman, M.S., Xu, B., Tsin, A. and Li, J. (2023) 'Laser-induced forward transfer (LIFT) based bioprinting of the collagen I with retina photoreceptor cells', *Manufacturing Letters*, Vol. 35, Supplement, pp. 477–484. doi: 10.1016/j.mfglet.2023.07.005.

Betancourt, N. and Chen, X. (2022) 'Review of extrusion-based multi-material bioprinting processes', *Bioprinting*, Vol. 25, e00189. doi: 10.1016/j.bprint.2021.e00189.

Brandman, J., Sturm, L., White, J. and Williams, C. (2020) 'A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems', *Journal of Manufacturing Systems*, Vol. 56, pp. 202–212. doi: 10.1016/j.jmsy.2020.05.014.

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G. and Ferrag, M.A. (2021) 'Cyber ranges and testbeds for education, training, and research', Applied Sciences, Vol. 11, No. 4, 1809. doi: 10.3390/app11041809.

Dou, C., Perez, V., Qu, J., Tsin, A., Xu, B. and Li, J. (2021) 'A state-of-the-art review of laser-assisted bioprinting and its future research trends', *ChemBioEng Reviews*, Vol. 8, No. 5, pp. 517–534. doi: 10.1002/cben.202000037.

Elgabry, M. and Johnson, S. (2024) 'Cyber-biological convergence: A systematic review and future outlook', *Frontiers in Bioengineering and Biotechnology*, Vol. 12, 1456354. doi: 10.3389/fbioe.2024.1456354.

Grijalva Garces, D., Strauß, S., Gretzinger, S., Schmieg, B., Jüngst, T., Groll, J., Meinel, L., Schmidt, I., Hartmann, H., Schenke-Layland, K., Brandt, N., Selzer, M., Zimmermann, S., Koltay, P., Southan, A., Tovar, G.E.M., Schmidt, S., Weber, A., Ahlfeld, T., Gelinsky, M., Scheibel, T., Detsch, R., Boccaccini, A.R., Naolou, T., Lee-Thedieck, C., Willems, C., Groth, T., Allgeier, S., Köhler, B., Friedrich, T., Briesen, H., Buchholz, J., Paulus, D., von Gladiss, A. and Hubbuch, J. (2024) 'On the reproducibility of extrusion-based bioprinting: Round robin study on standardization in the field', *Biofabrication*, Vol. 16, No. 1, 015002. doi: 10.1088/1758-5090/acfe3b.

Gupta, D., Derman, I.D., Xu, C., Huang, Y. and Ozbolat, I.T. (2025) 'Droplet-based bioprinting', *Nature Reviews Methods Primers*, Vol. 5, No. 1, 25. doi: 10.1038/s43586-025-00394-y.

Hadlington, L. (2017) 'Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours', *Heliyon*, Vol. 3, No. 7, e00346. doi: 10.1016/j.heliyon.2017.e00346.

Kallonas, C., Piki, A. and Stavrou, E. (2024) 'Empowering professionals: A generative AI approach to personalized cybersecurity learning', 2024 IEEE Global Engineering Education Conference (EDUCON), pp. 1–10. doi: 10.1109/EDUCON60312.2024.10578894.

Lévesque, M. and Tipper, D. (2016) 'A survey of clock synchronization over packet-switched networks', *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 4, pp. 2926–2947. doi: 10.1109/COMST.2016.2590438.

Liu, S., Kaur, N., Song, D.-H., Moses, J.C. and Ozbolat, I.T. (2026) 'Self-driving bioprinting laboratories', *Biofabrication*, Vol. 18, No. 1, 013001. doi: 10.1088/1758-5090/ae3645.

Malekpour, A. and Chen, X. (2022) 'Printability and cell viability in extrusion-based bioprinting from experimental, computational, and machine learning views', *Journal of Functional Biomaterials*, Vol. 13, No. 2, 40. doi: 10.3390/jfb13020040.

Matai, I., Kaur, G., Seyedsalehi, A., McClinton, A. and Laurencin, C.T. (2020) 'Progress in 3D bioprinting technology for tissue/organ regenerative engineering', *Biomaterials*, Vol. 226, 119536. doi: 10.1016/j.biomaterials.2019.119536.

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*, Vol. 6, 39. doi: 10.3389/fbioe.2018.00039.

Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., Song, J., Naik, I. and Fatema, K. (2026) 'Hacking the organism through digital technology: Exploring cyberbiosecurity vulnerabilities, threats, risks and their mitigations', in Naik, N., Jenkins, P., Prajapat, S. and Grace, P. (eds.) *Contributions Presented at the International Conference on Computing, Communication, Cybersecurity & AI: The C3AI 2025*. Lecture Notes in Networks and Systems, Vol. 1811. Cham: Springer, pp. 29–57. doi: 10.1007/978-3-032-16791-0_2.

Ng, W.L. and Shkolnikov, V. (2024) 'Optimizing cell deposition for inkjet-based bioprinting', *International Journal of Bioprinting*, Vol. 10, No. 2, 2135. doi: 10.36922/ijb.2135.

Palmer, X.-L., Akafia, C., Woodson, E., Woodson, A. and Potter, L. (2024) 'Organoids, biocybersecurity, and cyberbiosecurity—A light exploration', *Organoids*, Vol. 3, No. 2, pp. 83–112. doi: 10.3390/organoids3020007.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, Vol. 42, pp. 165–176. doi: 10.1016/j.cose.2013.12.003.

Pearce, H., Yanamandra, K., Gupta, N. and Karri, R. (2022) 'FLAW3D: A Trojan-based cyber attack on the physical outcomes of additive manufacturing', *IEEE/ASME Transactions on Mechatronics*, Vol. 27, No. 6, pp. 5361–5370. doi: 10.1109/TMECH.2022.3179713.

Piotrowska, U., Tsoi, J., Singh, P., Banerjee, A. and Sobczak, M. (2025) '3D bioprinting and artificial intelligence for tumor microenvironment modeling: A scoping review of models, methods, and integration pathways', *Molecular Pharmaceutics*, Vol. 22, No. 10, pp. 5801–5823. doi: 10.1021/acs.molpharmaceut.5c01062.

Pope, T. (2026) '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.

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.

Raeker-Jordan, N., Chung, J., Kong, Z.J. and Williams, C. (2024) 'Ensuring additive manufacturing quality and cyber–physical security via side-channel measurements and transmissions', *Journal of Manufacturing Systems*, Vol. 73, pp. 275–286. doi: 10.1016/j.jmsy.2024.02.005.

Reed, J.C. and Dunaway, N. (2019) 'Cyberbiosecurity implications for the laboratory of the future', *Frontiers in Bioengineering and Biotechnology*, Vol. 7, 182. doi: 10.3389/fbioe.2019.00182.

Rossel, J., Mladenov, V., Wördenweber, N. and Somorovsky, J. (2025) 'Security implications of malicious G-Codes in 3D printing', *Proceedings of the 34th USENIX Security Symposium*, pp. 1867–1885. Berkeley, CA: USENIX Association.

Sahoo, S., Dansana, D. and Mishra, B.K. (2020) 'Application and challenges of IoT in healthcare', in Mishra, B.K., Kuanar, S.K., Peng, S.-L. and Dasig, D.D. Jr. (eds.) *Handbook of IoT and Blockchain: Methods, Solutions, and Recent Advancements*. Boca Raton, FL: CRC Press, pp. 25–47. doi: 10.1201/9780367854744.

Schwab, A., Levato, R., D'Este, M., Piluso, S., Eglin, D. and Malda, J. (2020) 'Printability and shape fidelity of bioinks in 3D bioprinting', *Chemical Reviews*, Vol. 120, No. 19, pp. 11028–11055. doi: 10.1021/acs.chemrev.0c00084.

Sergis, V., Kelly, D.M., Pramanick, A., Britchfield, G., Mason, K. and Daly, A.C. (2025) 'In-situ quality monitoring during embedded bioprinting using integrated microscopy and classical computer vision', *Biofabrication*, Vol. 17, No. 2, 025004. doi: 10.1088/1758-5090/adaa22.

Shakil Arman, M., Xu, B., Tsin, A., & Li, J. (2023). Laser-induced forward transfer (LIFT) based bioprinting of the collagen I with retina photoreceptor cells. Manufacturing Letters, 35, 477–484. https://doi.org/10.1016/j.mfglet.2023.07.005

Shin, J., Lee, Y., Li, Z. et al. (2022) 'Optimized 3D bioprinting technology based on machine learning: A review of recent trends and advances', *Micromachines*, Vol. 13, No. 3, 363. doi: 10.3390/mi13030363.

Song, C., Lin, F., Ba, Z., Ren, K., Zhou, C. and Xu, W. (2016) 'My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3D printers', *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 895–907. New York, NY: Association for Computing Machinery. doi: 10.1145/2976749.2978300.

Sun, J., Yao, K., An, J., Jing, L., Huang, K. and Huang, D. (2023) 'Machine learning and 3D bioprinting', *International Journal of Bioprinting*, Vol. 9, No. 4, 717. doi: 10.18063/ijb.717.

Verizon (2024) *2024 Data Breach Investigations Report*. New York, NY: Verizon Business.

Wang, J., Cui, Z. and Maniruzzaman, M. (2023) 'Bioprinting: A focus on improving bioink printability and cell performance based on different process parameters', *International Journal of Pharmaceutics*, Vol. 640, 123020. doi: 10.1016/j.ijpharm.2023.123020.

Yamin, M.M., Katt, B. and Gkioulos, V. (2020) 'Cyber ranges and security testbeds: Scenarios, functions, tools and architecture', Computers & Security, Vol. 88, 101636. doi: 10.1016/j.cose.2019.101636.

Yampolskiy, M., King, W.E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A. and Elovici, Y. (2018) 'Security of additive manufacturing: Attack taxonomy and survey', *Additive Manufacturing*, Vol. 21, pp. 431–457. doi: 10.1016/j.addma.2018.03.015.

Zhang, D., Wang, Q.-G., Feng, G., Shi, Y. and Vasilakos, A.V. (2021) 'A survey on attack detection, estimation and control of industrial cyber-physical systems', *ISA Transactions*, Vol. 116, pp. 1–16. doi: 10.1016/j.isatra.2021.01.036.