The AI × Biosecurity Research Hackathon: Cross-Track Findings on DNA Screening, Early Warning, and Biosecurity Tools

Jason Hoelscher-Obermaier[1], Jaime Raldúa Veuthey[1], Kamil Alaa[1],
Joshua Landes[2], Grace Braithwaite[3], James Montavon[2]
[1]*Apart Research* [2]*BlueDot Impact* [3]*Cambridge Biosecurity Hub*
jason@apartresearch.com

1. Overview

The AI × Biosecurity Research Hackathon [1] (April 24–26, 2026) is a three-day open research event co-organized by Apart Research, BlueDot Impact, and Cambridge Biosecurity Hub, in a hybrid format combining online participation with regional in-person sites. We expect 100+ teams of researchers, engineers, and biosecurity practitioners to deliver research MVPs at the intersection of AI and biosecurity across four tracks aligned with CyberBio26's scope. By drawing from a broader pool than traditional biosecurity venues, hackathons can generate a broad range of independent solution approaches to provide insights on the relative tractability of different problems and the field's blind spots.

This submission proposes a two-part contribution to CyberBio26: (i) a short plenary talk summarizing cross-track findings from the event, and (ii) posters from top-performing teams showcasing concrete work from the sprint.

2. Tracks

Each track aligns with an active CyberBio26 topic of interest. All four are backed by domain sponsors who also contribute mentors and judges.

(1) DNA Screening & Synthesis Controls (sponsor: CBAI). Current DNA synthesis screening has known blind spots: sequence-similarity-based approaches, for instance, can miss AI-designed functional variants with low identity to catalogued pathogens. Participants build and evaluate screening tools, benchmark open-source screeners such as IBBIS Common Mechanism [2], and contribute defensive improvements upstream.

(2) Pandemic Early Warning (sponsor: Equistamp). Outbreak detection tools could flag anomalies days before clinical confirmation, but surveillance systems remain fragmented across institutions with limited data integration. Participants build AI-powered detection, data fusion, and alert systems using public epidemiological and environmental datasets.

(3) AI Biosecurity Tools (sponsor: Fourth Eon Bio). Defensive utilities for biosecurity workflows: risk-assessment systems, data integration pipelines, and accessible tooling for under-resourced institutions.

(4) Benchtop Synthesizer Security (sponsor: Sentinel Bio). Benchtop DNA synthesizers can now print sequences at the scale of small RNA viruses ($\sim$7 kb), with capabilities growing, but the hardware lacks built-in screening or tamper-resistant logging. Participants tackle on-device security, fragment-assembly detection, and split-order monitoring.

3. Judging and Dual-Use Safeguards

Each submission is a research MVP consisting of a short write-up plus code and data if applicable. A panel of 40+ judges from biosecurity and AI safety organizations scores submissions on novelty, impact, rigor and clarity of presentation. Prizes total $6,000 and top-ranked teams are invited to The Apart Fellowship or the CBAI Fellowship fast-track to continue the work after the sprint.

Dual-use safeguards are built into the event design. Submissions are reviewed for information hazards before public dissemination; code and data flagged as lowering barriers to misuse are restricted from open release. The organizing team ruled out proposed tracks that would have directly stress-tested biosafety measures. The event includes a session on responsible disclosure norms and information-hazard awareness.

4. Previous Experiences

This is the second iteration of a hackathon-to-workshop pipeline we have run. In January 2026, Apart ran an AI Manipulation research hackathon [3] in coordination with the organizers of a workshop on AI manipulation (AIMII) at the IASEAI conference in Paris. That hackathon drew 500+ participants who submitted 70 projects across 26 countries. The top projects were invited to present posters at the AIMII Workshop in February 2026 [4], accompanied by an overview of the event in a panel discussion. The format worked well and surfaced valuable contributions in understudied parts of AI manipulation research, which is why we are proposing the same pattern for CyberBio26.

5. Proposed CyberBio26 Contribution

We propose:
(i) A plenary talk covering motivation, track design, headline findings from each track, lessons from running an open event on dual-use topics, and follow-on work for top projects.
(ii) Three posters from top-ranked hackathon teams. Poster presenters will register for and attend CyberBio26 in person.

The tracks target several CFP topics directly: DNA Synthesis and Screening Security (tracks 1 and 4); AI Safety in Biotechnology, covering adversarial attacks on ML models in biological applications and information-hazard management (track 1 and the event's dual-use safeguards); Threat Detection and Response, covering anomaly detection in biological data streams (track 2); and Regulatory and Policy Frameworks, covering risk assessment and dual-use considerations (track 3). The deliverable to CyberBio26 is a set of new research results from a broad, fast-moving contributor pool, plus organizational lessons from running an event of this kind.

References

[1] AI × Biosecurity Research Hackathon, April 24–26, 2026. https://apartresearch.com/sprints/aixbio-hackathon-2026-04-24-to-2026-04-26

[2] IBBIS Common Mechanism. https://ibbis.bio/common-mechanism

[3] AI Manipulation Research Hackathon, January 9–11, 2026. https://apartresearch.com/sprints/ai-manipulation-hackathon-2026-01-09-to-2026-01-11

[4] AIMII Workshop on AI Manipulation, IASEAI Conference, Paris, February 26, 2026. https://aimii.info/