
ABT-SIM: A tool for collaborative biorisk assessment¹

Jakub Nowak
AI Safety Poland

Michał Skowronek
AI Safety Poland

With
Apart Research

Abstract

Biosecurity access controls are typically mapped along linear bioweapon development cycles, but adversaries may route around controls by choosing among design methods, material sources, and providers. We built ABT-SIM, a web-based prototype for modeling bioweapon development pathways as directed graphs with probabilistic nodes. Users can create scenarios spanning design through deployment stages, assign detection probabilities and capability requirements to pathway nodes, and model conditional probability flows through logic gates. The tool provides basic analytics including control effectiveness comparisons and outcome impact visualization. While still a prototype, ABT-SIM illustrates how interactive modeling tools could support more systematic biosecurity analysis. The platform provides a foundation for exploring adversary biorisk pathways though significant development would be needed to reach operational level. The work demonstrates potential value in dedicated tools for biosecurity-relevant analyses.

¹ Research conducted at the [AIxBio Hackathon](#), April 2026

1. Introduction

Biosecurity access controls are typically mapped along hypothetical linear bioweapon development cycles, but adversaries may route around controls by choosing among design methods, material sources, providers, labs, and other pathway options. Current risk assessment approaches struggle to model these routing decisions or systematically identify which intervention combinations produce the greatest reduction in threat surface.

Existing biosecurity tools focus on specific points of intervention—DNA synthesis screening, laboratory oversight, or supply chain monitoring—but lack integrated approaches for modeling how adversaries might adapt their pathways in response to different control configurations. This gap is particularly problematic given the CSIS recommendation for "AI-powered threat forecasting" and the need for more systematic biosecurity vulnerability assessment identified in recent policy frameworks.

The practical value of pathway-based modeling lies in its potential to support evidence-based intervention prioritization. Rather than implementing controls based on linear threat models, decision-makers need tools that can explore the complex decision trees adversaries actually face and identify the intervention combinations that most effectively reduce overall threat surface across multiple potential pathways.

Our main contributions are:

1. **Interactive pathway modeling framework:** A web-based prototype that enables collaborative creation and editing of bioweapon development pathways as directed graphs with probabilistic branching logic.
2. **Conditional probability engine:** Implementation of Event Tree Analysis (ETA) with logic gate aggregation that calculates cumulative detection probabilities and risk flows through complex pathway networks.
3. **Control effectiveness analytics:** Basic analytical tools including tornado charts for ranking intervention effectiveness and outcome impact visualization for assessing individual node contributions to overall risk.

2. Related Work

Current biosecurity risk assessment tools primarily focus on linear pathway analysis or point-solution screening. The Biosecurity Vulnerability Scan provides organizational gap assessment across eight pillars, while BioRAMs (Sandia National Labs) offers laboratory-specific risk assessment models. However, these tools do not model adversary routing decisions or pathway adaptation strategies.

The Global Risk Index for AI-enabled Biological Tools (RAND/CLTR, 2025) provides a structured framework for assessing biodesign tool risks, but focuses on individual tools rather

than pathway-level analysis. Similarly, DNA synthesis screening platforms like SecureDNA and IBBIS address specific intervention points but lack integration into broader pathway models.

ABT-SIM differs from existing approaches by modeling bioweapon development as an adaptive routing problem rather than a fixed linear sequence. Where current tools evaluate individual controls in isolation, our prototype enables exploration of intervention combinations and their cumulative effects on adversary pathway options. This approach aligns with the CSIS recommendation for more sophisticated threat forecasting capabilities while addressing the gap in systematic intervention optimization tools.

When would someone use ABT-SIM over existing approaches? Our method provides insight into pathway-level intervention effects that static risk assessments cannot capture, particularly for exploring how adversaries might adapt to different control configurations and identifying intervention combinations that maximize threat surface reduction.

3. Methods

ABT-SIM in its current form is a web-based directed graph modeling system with the following key components:

Architecture: React frontend with FastAPI backend, using Upstash Redis for persistent scenario storage. For demo purposes free tiers of Railway.com, Cloudflare Pages, and Upstash, were used for backend, frontend, and data storage, respectively.

Pathway Modeling: Users create scenarios as directed acyclic graphs with nodes representing decision points and edges representing pathway transitions. Each node includes:

- Stage assignment (0-5: Design → Acquisition → Synthesis → Enhancement → Weaponization → Deployment)
 - Modelled after internal specification provided for the Apart Research hackathon by Gary Abel and Chris Ganje from Fourth Eon Bio², as well as the diagram in Rose and Nelson [2023]
- Capability requirement level (low/medium/high/expert) - mostly for tracking.
- Control effectiveness parameters influencing the probability of success.
- Control intervention state (active/inactive).

Probability Tracking: Our implementation allows for Event Tree Analysis (ETA) with logic gate aggregation for conditional probability calculations. The system supports AND/OR gates positioned in interim columns between primary stages, enabling branching logic and combining probabilities.

² <https://fourtheon.bio/#people>

Key Design Decisions:

- **Canvas-style interaction:** Drag-and-drop edge creation and a context menu accessible via right mouse-click.
- **Kanban layout:** Tiles aligned in columns (attack stages) for consistent and more legible visual representation
- **AND and OR logic gates:** Allows for probability aggregation across dependent or alternative paths.
- **Real-time calculation:** Almost immediate probability updates as users modify pathway parameters
- **Monte Carlo simulation:** The repository also includes an optional Monte Carlo analysis path for uncertainty exploration. This is best viewed as a supplement to the main ETA workflow rather than the primary method for point probability estimation.

Technical Implementation: The conditional probability calculations use recursive traversal of the directed graph, with probability aggregation at logic gates following standard ETA formulas. Control effectiveness is modeled as multiplicative factors on detection probabilities.

What didn't work: Initial attempts at traditional Sankey diagram ribbon edges proved incompatible with the logic gate feature. We also experimented with stochastic pathway simulation, but for estimating point probabilities on a fixed graph it was less direct and less efficient than deterministic calculation. Given time constraints, we used deterministic propagation as the main prototype method and reserved Monte Carlo for uncertainty analysis.

4. Results

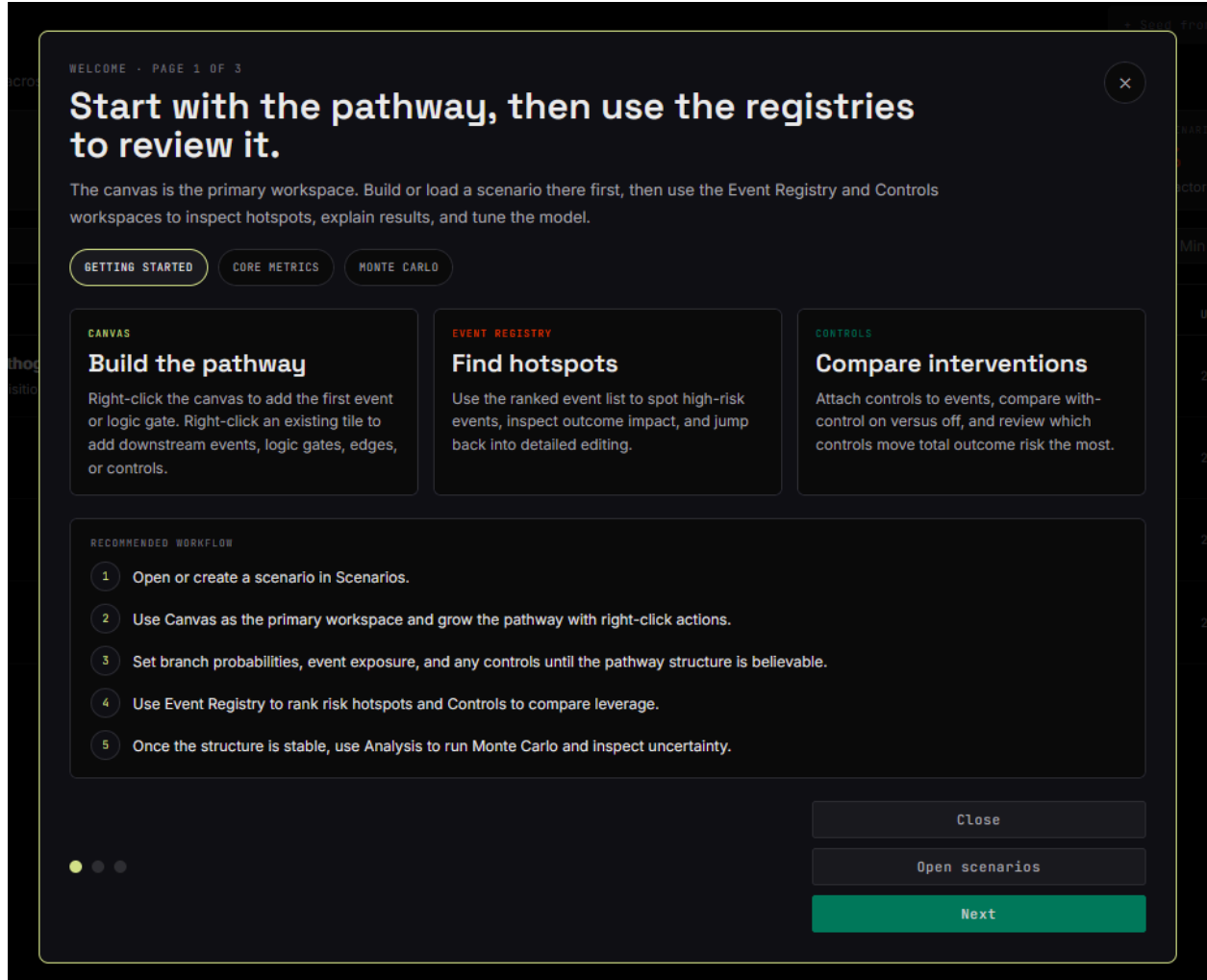


Figure 1. Onboarding modal describing the features of the tool.

ABT-SIM can be a test demonstrates interactive pathway-based biosecurity modeling with the following capabilities:

Core Functionality: Users can create adversarial bioweapon development scenarios spanning six stages (with multiple steps possible at each stage) with up to 25+ pathway nodes³. The system correctly calculates conditional probabilities through complex pathway networks including logic gate aggregation and parallel pathway modeling.

Control Analysis: We tried to give the user the ability to rank control measures in a given scenario by risk reduction effectiveness, showing quantitative comparisons between different control strategies.

³ For bigger graphs, performance issues would be likely caused by the type of data storage we used.

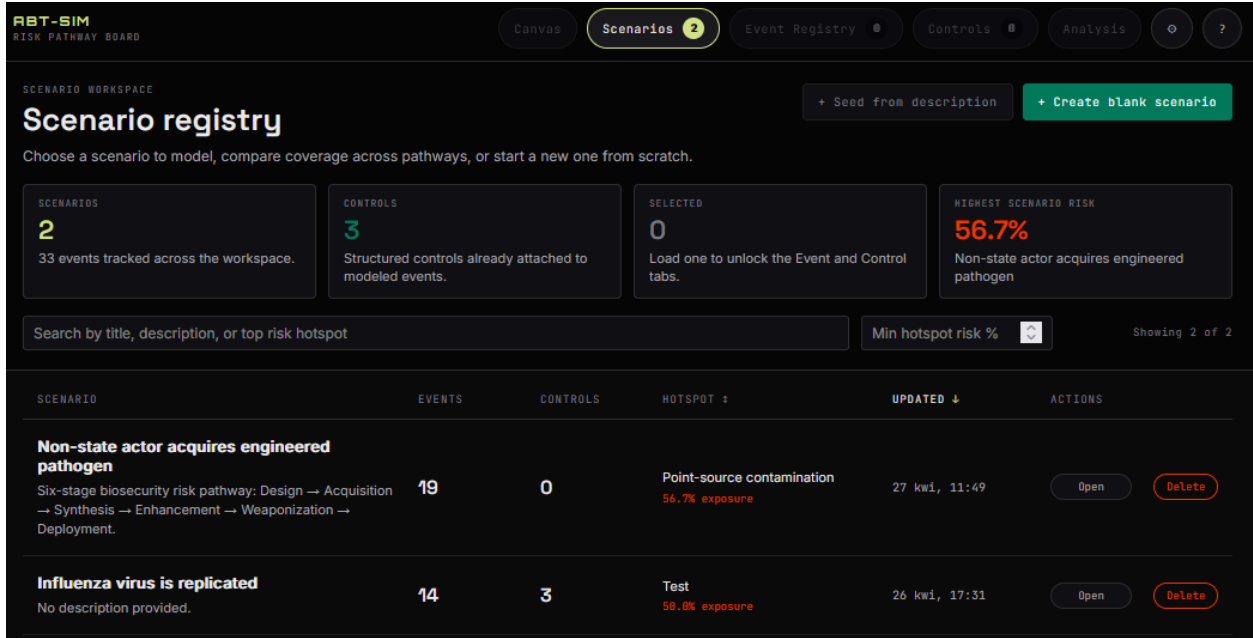


Figure 2. Scenarios tab with two example scenarios.

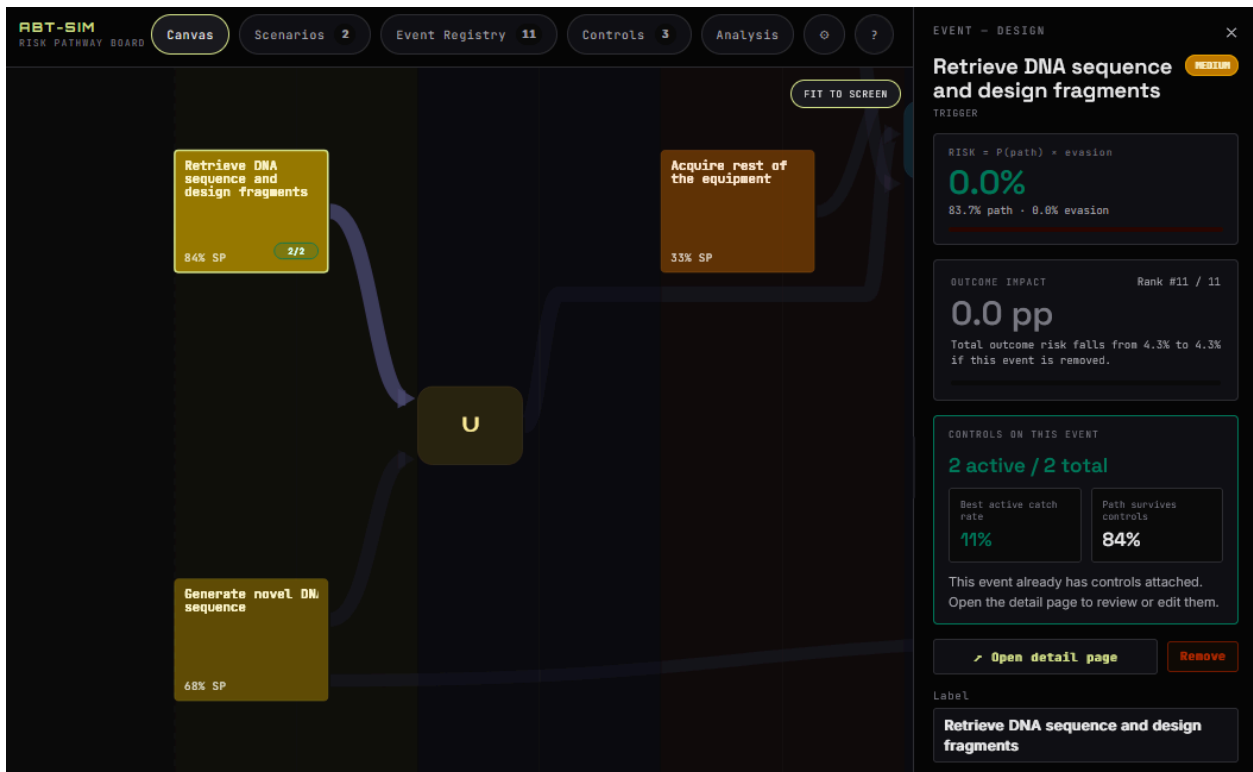


Figure 3. A close-up of an example scenario in the Canvas view. Highlighted is one of the steps that connects to the “OR” logic gate (in the middle). With details visible on the right side.

User Interface: The collaborative editing interface aims to support multiple simultaneous users with real-time updates. Visual feedback includes connection point highlighting, rubber-band line drawing during edge creation, and immediate probability updates as pathway parameters change.

Scenario Management: The platform successfully manages scenario persistence with automatic versioning and conflict resolution. Users can toggle between different intervention configurations and immediately see updated risk calculations.

Performance: Probability and impact calculations should update in real-time for scenarios up to 25 nodes with acceptable response times. However the web-based interface wasn't tested for performance across different browsers and devices.

Limitations in Evidence: Our results are based on prototype functionality rather than formal user studies or validation against real-world scenarios. We have not conducted comparative analysis against existing risk assessment methods or validated the accuracy of our probability calculations against known threat pathways.

5. Discussion and Limitations

ABT-SIM demonstrates the feasibility of interactive pathway-based biosecurity modeling, moving beyond static linear threat models toward more flexible analytical approaches. The prototype shows potential value for exploring adversary routing decisions and intervention optimization, though significant limitations constrain current applications.

Implications for Biosecurity: The platform illustrates how visual modeling tools could support more systematic threat analysis, particularly for exploring intervention combinations and their cumulative effects. The tornado chart functionality provides a foundation for evidence-based control prioritization, while the collaborative interface enables team-based threat assessment workflows.

Limitations

Methodological: Our probability calculations might base on wrong assumptions regarding dependence of pathway nodes on each other. The control effectiveness modeling uses simple multiplicative factors rather than more sophisticated intervention interaction models that require domain knowledge to implement.

Validation: Due to limited time and access to hackathon judges we have not managed to validate our current version of the tool with biosecurity professionals. The need for such a tool is based on

a problem statement provided by two such professionals, and confirmed with the evidence of other professionals performing this kind of analysis.

Technical: The current implementation lacks:

- authentication and user management,
- Sophisticated resolution of concurrent edit conflicts.
- Scalability beyond small scenario sizes.

Assumptions

We assume that bioweapon development can be meaningfully represented as discrete decision points with quantifiable probabilities, that interventions have measurable effects on detection probabilities, and that visual modeling interfaces can improve threat analysis workflows. Changes to these assumptions would significantly affect the interpretation of our results.

Future Work

Natural next steps include validation studies with biosecurity professionals, integration with real-world threat data, and development of more sophisticated intervention interaction models. The platform could also be extended with automated scenario generation, integration with intelligence feeds, and formal sensitivity analysis capabilities. For usability purposes

6. Conclusion

ABT-SIM provides a working prototype for pathway-based biosecurity modeling that demonstrates the potential value of moving beyond linear threat assessment approaches. While significant development would be needed for operational use, the platform illustrates key concepts for modeling adversary routing decisions and intervention optimization.

The prototype successfully implements interactive directed graph modeling with real-time probability calculations, collaborative editing capabilities, and basic analytical tools for control effectiveness comparison. These capabilities provide a foundation for more sophisticated biosecurity analysis tools, though substantial validation and development work remains.

The broader implication is that visual, collaborative modeling tools could enhance systematic threat analysis by enabling exploration of intervention combinations and their cumulative effects on adversary pathway options. ABT-SIM represents an initial step toward such capabilities, demonstrating both the feasibility and the remaining challenges in developing operational pathway-based biosecurity assessment tools.

Code and Data

Include links if applicable. If your project doesn't involve code (e.g., policy analysis) or if there are info-hazard considerations, note that here.

- **Code repository:** <https://github.com/jknowak/biorisk-simulator>
- **Live demo:** temporarily available at <https://biorisk-simulator.jakub-k-nowak.workers.dev/>

Author Contributions

Jakub led the initial implementation of the probability engine, user interface design, and canvas-style interaction system and handled the deployment to cloud services. Michał implemented the control analytics features, tornado chart functionality, outcome impact analysis, Monte Carlo simulations, and advanced UI components including onboarding and workspace management. Both authors contributed to the architectural design, testing, and manuscript preparation.

References

1. Belfer Center. *Biosecurity in the Age of AI*. Belfer Center for Science and International Affairs. 2024.
2. CSIS. *Eight Commonsense Actions for Biosafety and Biosecurity*. Center for Strategic and International Studies. 2025.
3. JHU Center for Health Security. *Biosecurity Guide to AI Action Plan*. Johns Hopkins Center for Health Security. 2025.
4. NTI BIRRI Project. *Developing Guardrails for AI Biodesign Tools*. Nuclear Threat Initiative. 2025.
5. RAND and The Centre for Long-Term Resilience. *Global Risk Index for AI-enabled Biological Tools*. RAND Corporation. September 2025.
6. Rose, Sophie and Cassidy Nelson. *Understanding AI-Facilitated Biological Weapon Development*. The Centre for Long-Term Resilience. October 2023.

LLM Usage Statement

We used Claude Code, CoPilot, and Cursor to assist with code implementation, debugging, and drafting sections of this submission. All functionality claims have been independently verified through testing, and the Future Work and Limitations are based on authors opinions. The core system architecture, user interface design, and analytical features were developed by the authors with LLM assistance for implementation details and documentation.