FT: Expanding XR Attack Surface

2026 FT: Expanding XR Attack Surface

Card Type	Future Technology Possibility
Series	Immersive Futures Guild — Vision 2035
Layer	1 — Atomic Foresight Object
Status	Active
Confidence	Medium
Workshop	Circle of Scholars — January 2026
Facilitator	Circle of Scholars Workshop Team
Tags	cybersecurity | attack-surface | privacy | layer1 | ft
Tally.so Form	https://tally.so/r/ilrn-if-ft-xratk-2026

As immersive environments become more interconnected and data-rich, they become larger and more consequential targets for malicious actors. The XR attack surface includes hardware vulnerabilities, platform data breaches, identity spoofing in social VR, manipulation of environmental stimuli to induce disorientation or harmful responses, and exfiltration of biometric and behavioral data.

Key Drivers / Contributing Conditions:

- Increasing value of biometric data to malicious actors
- Complexity of multi-platform XR environments creating security gaps
- Limited security culture in EdTech development pipelines

Tensions Carried Forward to Part II:

- How should security threat modeling be integrated into pedagogical design processes?

- What liability frameworks apply when an educational XR platform is exploited to harm learners?

Linked Scenarios / Strands: SC: Ethics Privacy & Bodily Autonomy | SCENARIO: Extractive Surveillance

Ways of Knowing: Tree · Garden · Lantern

PART II — COMMUNITY EVIDENCE & DIALOGUE TRACK | FT: Expanding XR Attack Surface | H2 2026 — Living

T	COMMUNITY CONTRIBUTION FORM — FT: Expanding XR Attack Surface Submit case examples, methodological challenges, cultural perspectives, and proposed evidence criteria via: https://tally.so/r/ilrn-if-ft-xratk-2026

Part II — Scope and Instructions
This section collects community responses, case examples, and challenges to the Part I foresight snapshot above.
It opens July 1, 2026 and undergoes synthesis review in September 2026, November 2026, and January 2027.
Contributions are submitted via the Tally.so form above and appear in the registers below after editorial review.
The Part I text is not modified in response to Part II contributions; it is versioned at the Annual Handoff review.
Contribution categories: Case Example | Methodological Challenge | Cultural/Community Perspective | Proposed Evidence Criterion
Ways of Knowing accepted: Tree (evidence) | Garden (practice) | Lantern (futures)

Tensions Open for Community Response:

- How should security threat modeling be integrated into pedagogical design processes?
- What liability frameworks apply when an educational XR platform is exploited to harm learners?

Contributor / Date	Category	Way of Knowing	Contribution Summary
[Awaiting contributions — form opens July 1, 2026]			

Revision #1
Created 25 May 2026 20:30:24 by Jonathon Richter
Updated 25 May 2026 20:31:24 by Jonathon Richter