



PERSLIS DEFENSE · 种子轮

自适应的自主。固定的权限。

一个无权重的机器大脑：从自己的失败中写下规则，在机器本地运行、不依赖网络链路，并接入你已经列装的系统——在人的指挥之下。

融资 500-1000 万美元 · 24 个月资金跑道 · 5-7 人团队

自主正在规模化到来。现有的“大脑”并不是为战场打造的。

规模是既定计划

2023 年 8 月宣布的 Replicator 计划，目标是在 18 到 24 个月内跨多个领域列装数以千计的可消耗自主系统。

美国国防部副部长，2023 年 8 月

神经模型是冻结的

上线前训练好，回到数据中心重新训练，依赖数据链或大型 GPU，说不清原因——而且对齐的是厂商的政策，不是你的命令。

部队运行在老旧系统之上

一套协调国家核力量的系统运行在 1970 年代的 IBM Series/1 上，使用 8 英寸软盘；约 75% 的联邦 IT 支出用于维持现有系统运行。

GAO-16-468, 2016

Peel: 一个无权重模型，采用失败优先架构。

传感器

→ 眼

→ PEEL

→ 地板

→ 追踪

→ 执行器

无权重

里面没有神经网络。它知道的是你能打开阅读的显式状态和规则。

失败优先

失败就是输入。它在任务途中、在机器上学习——没有训练过程，没有数据中心。

一个密封的大脑

一个签名文件，每次运行前校验。换一副身体只需要新的适配器。

它自己写规则。无需有人维护。

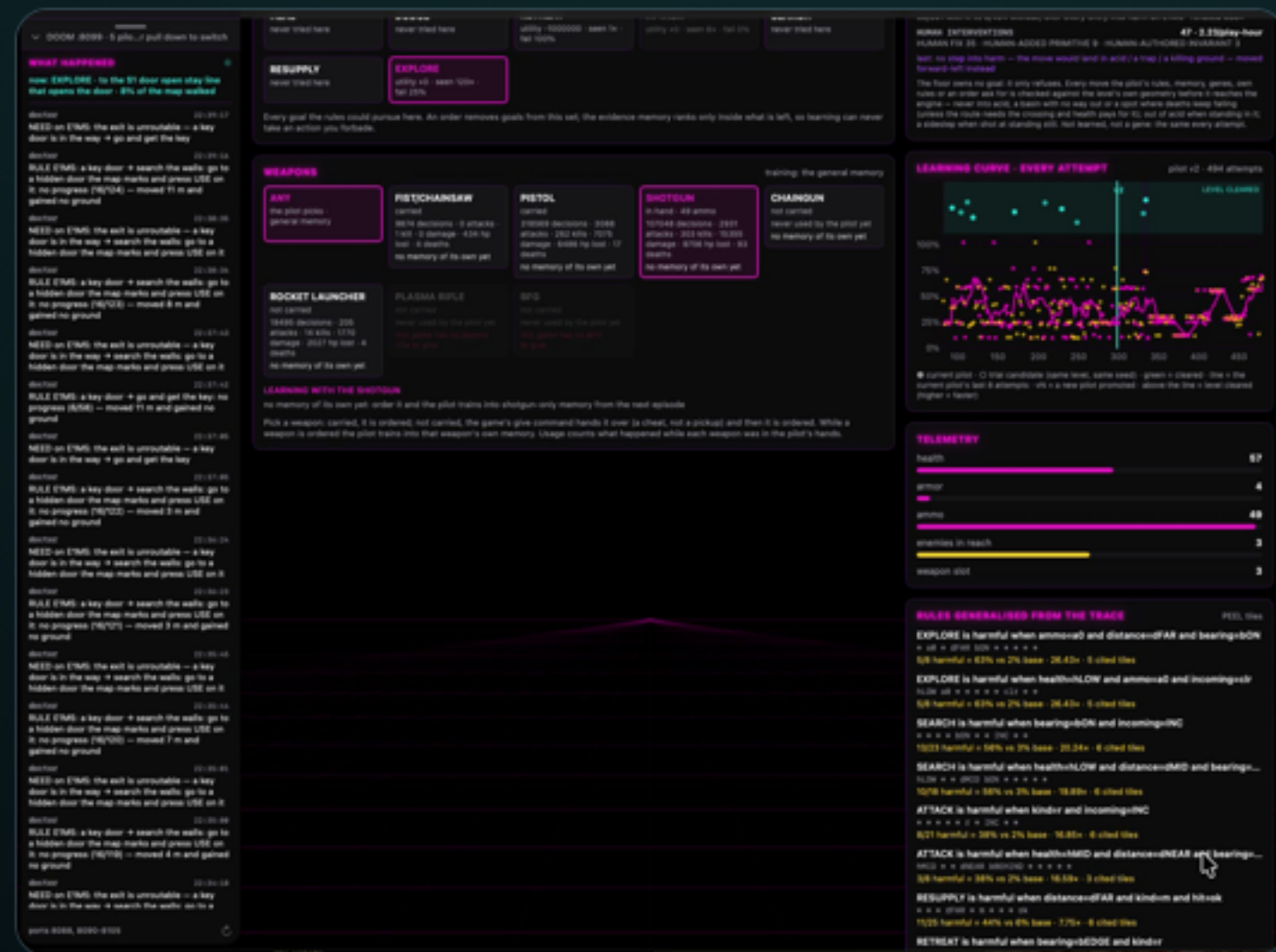
- 每一次失败都被记录并解释。
- 它提出一个改变，与老办法在同一关卡、同一种子上正面对打。
- 只有明显胜出 ($z \geq 2$) 才保留；输了就扔掉。然后用平实的语言写下来，附上赢得它的那些失败。

1 / 37

它在 DOOM 中为自己提出、最终保留的改变

80 → 15

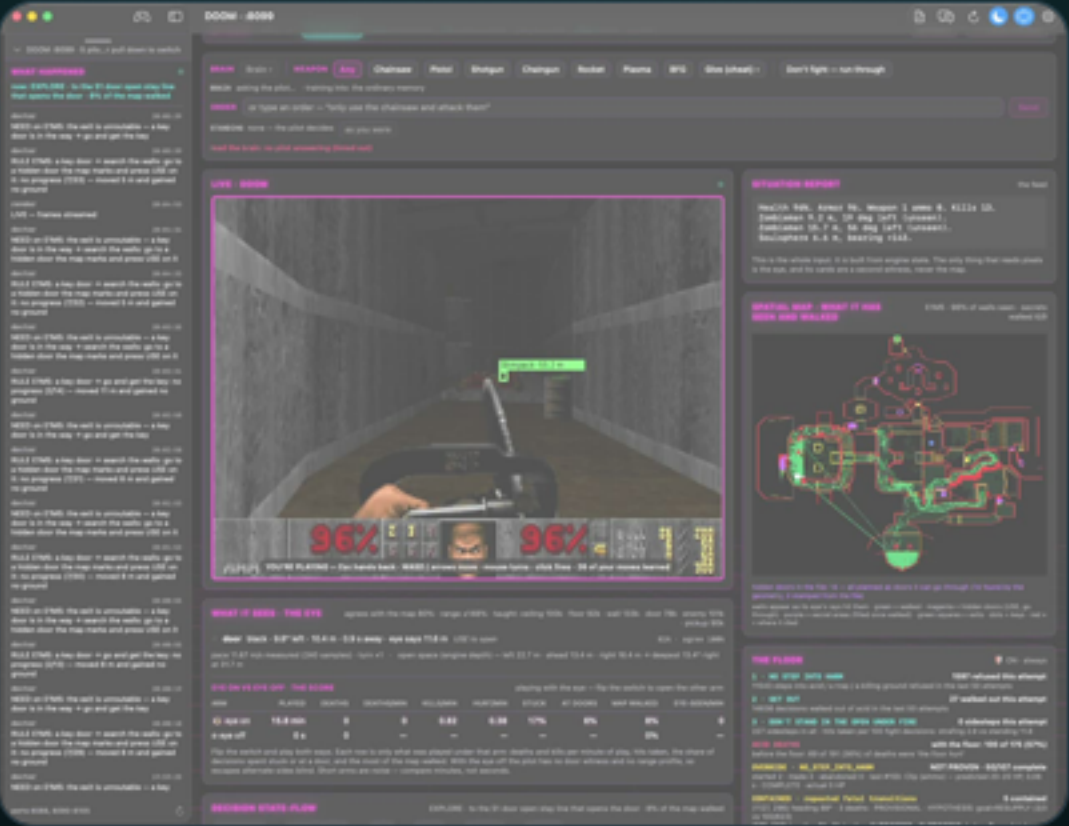
Fallout 中每小时死亡次数，学习关 vs 开，同一存档与种子



证据： 防御与进攻，失败一并列出。

测试	结果	对我们不利的
敌意驾驶控制器	64,952 条坏指令全部覆盖，0 碰撞	是边界，不是学习
无人机航线，未见起点	10/10 无碰 vs 全新 0/10	2-3 米/秒追击会坠毁
坦克大脑移入新游戏	+17%；修剪后 +66%	第二次导出只打平
BattleZone	27,000，随机为 3,000	一条闪避规则被否决
DOOM E1M1, Hurt Me Plenty	52 秒到达出口	Nightmare 未通关
3D 坦克竞技场	每分钟净击杀 -1.17 → -0.26, 从手写到演化	仍输给游戏自带 AI

全部在游戏与仿真中测量，并连同样本量公开。



你愿意让聊天机器人开你的坦克吗？

驾驶者，一场 10 分钟比赛	击杀 – 死亡
游戏自带 AI（多年调校）	38 – 6
我们的规则驾驶员	20 – 20
DeepSeek	10 – 18
Claude，每个决定 7.6 秒	1 – 15
Llama 3.2 3B	0 – 10

- 8 个坦克情境的笔试：Peel 8/8，Claude 6/8，DeepSeek 5/8。
- 通用模型听命于厂商政策，需要数据链或 GPU，还可能自信地编造。
- 如实说明：一场比赛；Claude 通过命令行工具运行；游戏自带 AI 也打赢了我们。

所有端点，接进一个大脑——包括没有 API 的。

老软件，没有 API

通过它自己的按钮、字段和屏幕驱动，留有收据。已在 Windows 95 到 11 的隔离副本中展示。

服务器与主机

通过它们已有的入口。COBOL 答案由编译器证明，否则拒绝。

你的失败，它的规则

失败遥测变成下一个系统的规则。已用公开记录做过一次：8,219 份联邦撞车报告 → 15 条驾驶规则，6 条已执行。

不用推倒重来，也不用新的采购项目。尚未展示：军用总线（MIL-STD-1553、ARINC 429、CAN）或任何已列装系统。

对齐的是指挥官，不是模型。

人

设定权限、命令和交战规则。对武力的使用行使判断。

地板

一个确定性机制，执行由授权政策、任务规则、安全限制和适用交战规则转化而来的机器可读约束。它学到的任何东西都不能放宽它们。

- 每个决定都留下书面理由——战后复盘可重放，同样的事实，同样的决定。
- 朝美国国防部第 3000.09 号指令推进：“对武力的使用行使适当程度的人类判断”。

为什么它能在神经自主吃力的地方胜出。

成本

不需要 GPU 集群，不需要训练。大脑在平台自己的计算机上运行。

可保证性

确定、可重放：拥有黑盒没有的测试与认证路径。

现场学习

在任务途中从出错之处学习，无需送回后方、无需承包商。

迁移

一个大脑跨平台；适配器是唯一的新代码。

遗留系统覆盖

连接永远不会有 API 的系统。

你已拥有的数据

你的失败遥测就是训练集——而且它仍然归你所有。

它接入哪里，如何赚钱。

谁来用

- 打造无人空中与地面系统的主承包商和集成商。
- 需要可重放决策的项目办公室与测试评估团队。
- 没有 API 的遗留系统的保障。

如何赚钱（计划）

- 按平台类型收取大脑许可费。
- 集成：通往你机器与遗留端点的适配器。
- 评估合同：在你录制的任务上做影子模式研究。
- 通过 SBIR/STTR、OTA 以及与主承包商合作进入。

尚无收入，尚无合作方集成。

24 个月，一次过一道关。

0-6 月

真实飞控在环 · 首个合作方影子模式

6-12 月

廉价地面与空中机器人仅用自身传感器 · 首个合作方集成

12-18 月

工作台上的人形机器人 · 军用总线适配器

18-24 月

擂台：经认可的机器人对机器人比赛 · 独立测试协议移交

每一步开始前都写好过关标准；没有测到的结果，就不往前走。24 个月之后：受人指挥、具备作战能力的人形平台。

这是计划，不是结果。目前只有仿真与游戏部分已建成。

5-7 人的团队。刻意精简。

创始人 / 架构师

大脑、地板、演化器

自主系统工程师

运行时、适配器、实时

机器人与硬件在环工程师

飞控、机器人、人形机器人

遗留集成工程师

无 API 系统、主机、总线

测试评估负责人

过关标准、协议、独立测试

安全与合规

CMMC 路径、出口管制、供应链

项目与合作

主承包商、项目办公室、SBIR/OTA

创始人已就位；其余为招聘计划。不需要 GPU 团队：大脑没有需要训练的权重。

我们的请求：500-1000 万美元，24 个月。

资金用途（计划）



区间两端各买到什么

- **500 万美元：**核心团队、硬件在环、低成本机器人、首个合作方先影子模式再集成。
- **1000 万美元：**以上全部，再加人形机器人项目与擂台、军用总线适配器、第二个合作方，以及独立验证。

风险，以及每一个如何被化解。

风险	如何化解
迁移并非自动（第二次导出只打平）	每一步都有书面关口；未测量的结果不推进
危险与目标同路时，谨慎会丢分（Freeway -12%）	这类限制由人事先设定；大脑学战术，不学权限
眼睛的余量很薄	它弃权而不是猜；6-12 月获得更多真实传感器数据
尚未列装	先影子模式：只记录本会做什么，什么都不碰
政策与信任	人对武力的判断、确定性的地板、每个决定可重放的追踪

为什么主承包商应该参与这一轮。

- 一个大脑，适用于你已经在打造的平台——空中、地面、遗留系统——每个平台只需一个适配器。
- 一份你的测试评估团队可以重放的决策记录，一个你的项目办公室能读懂的地板。
- 你的失败遥测变成你拥有的规则，而不是你租来的权重。
- 一支小团队，一份带书面关口的 24 个月计划，结果连同失败一起公开。

联系我们 → [Perslis 国防](#) →