

OCTOBER 2026

Neuromorphic AI moves the attack surface into the device

What changes for cybersecurity when AI runs on events, inside physical things, and keeps learning.

Terence Kok **with** Maria Singh

From clocked software to event-driven chips that can learn

AI AS SOFTWARE	AI ON A NEUROMORPHIC DEVICE
Code and fixed weights	Weights plus the timing of events
Changes only through a release	Can change on the chip as it learns
Inputs are data and prompts	Inputs include light, motion and sound
Sits behind access control	Often within public reach

1.15bn

neurons in Intel's Hala Point, on 1,152 Loihi 2 chips

Delivered to Sandia National Laboratories in 2024. At the other end, BrainChip's Akida Pico core draws under a milliwatt. Intel; BrainChip.

Four routes into an event-driven device

- 1 Sensor input: light, flicker, motion
- 2 Side channel: power, timing, EM
- 3 Fault injection: power and laser glitches
- 4 Learning: teaching the device the wrong thing

100%

attack success for flashing-light backdoors on event cameras

Up to that figure in the Flashy Backdoor study, with common defences often failing. Power and laser faults cut accuracy by up to 85.65%. Riaño et al., 2024; Nagarajan et al., DATE 2022.

The usual security tools do not reach the chip

GAP

No endpoint agent or scanner for a spiking processor

GAP

A flaw in a trained model may never get a CVE

GAP

Learned behaviour cannot be patched, only retrained or rolled back

GAP

The chip arrives inside a camera, not on the AI register

“A year after approval, the risk assessment describes a device that no longer exists.”

The EU AI Act (Art. 43(4)) and the FDA's change control plans already answer this: set the limits of change in advance.

A learning envelope for every adaptive device

WHAT	Which parts of the model may change
HOW FAR	The size of change allowed before review
TEST	A regular challenge test on the device
TRIGGER	Learning suspended when a limit is breached
RESET	A protected copy of the approved model
OWNER	A named owner signs off any change

Five questions for the board

- 1** Which devices carry AI that learns?
- 2** Where is each learning envelope?
- 3** When did we last re-test them?
- 4** Does the threat model cover light and power?
- 5** Can every device be put back?

Govern how far each device may **change**.

Write the limits down, test against them, and keep a way to put the device back.



Terence Kok with Maria Singh

SAVE · COMMENT · FOLLOW