

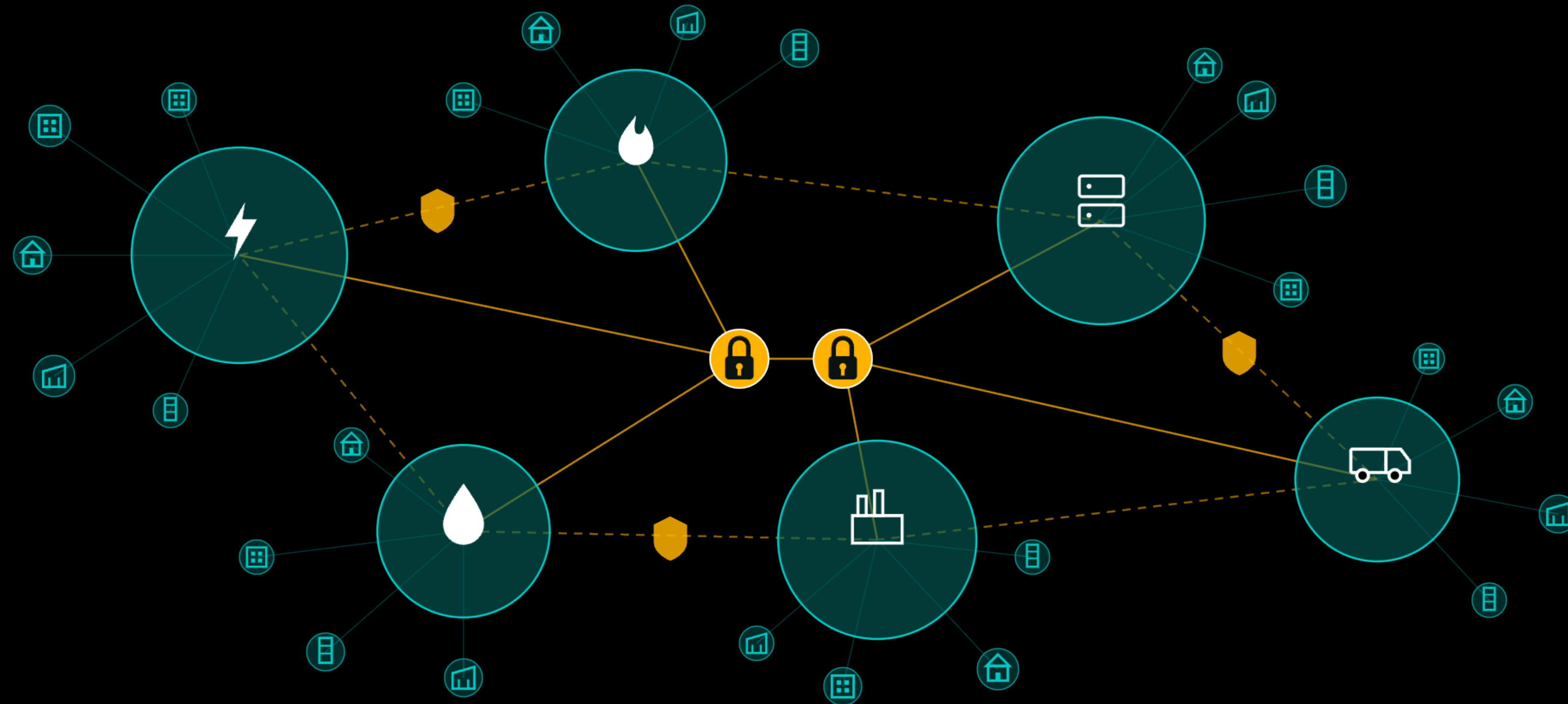
THE NEXT THREE YEARS OF xOT DEFENSE

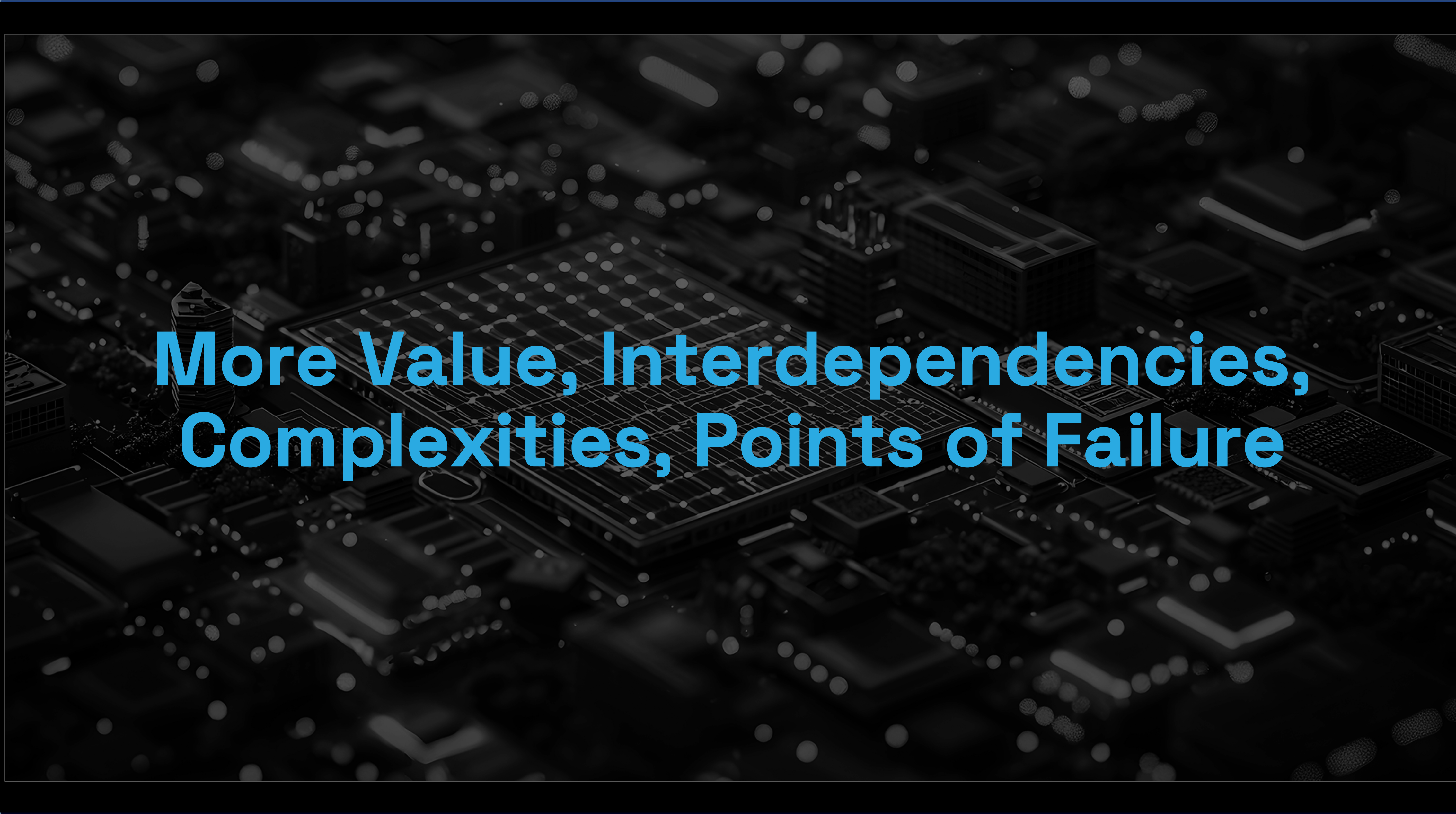
ROBERT M. LEE
CEO AND CO-FOUNDER, DRAGOS



We Have Moved to x0T

Environments Are Becoming Homogenous With a Technology Overlay



The background of the slide is a dark, high-angle aerial photograph of a city at night. The city's lights are blurred into bokeh, creating a sense of depth and complexity. A faint, glowing grid pattern is overlaid on the city, suggesting a digital or data-driven environment. The overall color palette is dark with blue and white highlights.

More Value, Interdependencies, Complexities, Points of Failure

A black and white photograph of a man wearing a white hard hat and a high-visibility safety vest. He is holding a tablet computer and looking at it intently. He is standing in a server room, with rows of server racks visible in the background. The lighting is dim, with some light coming from the racks and the ceiling. The overall tone is professional and technical.

AI: Inside the Control Loop and Supporting Human Decisions



While We Struggle with Root Cause Analysis

ICS Attack Capabilities Are Now Commodity

Moderately skilled adversaries can now acquire or develop tools threatening operational integrity

Public Protocol Libraries

- Modbus, DNP3, S7comm freely available
- No specialized knowledge required

Working Attack Tools Observed in 2025

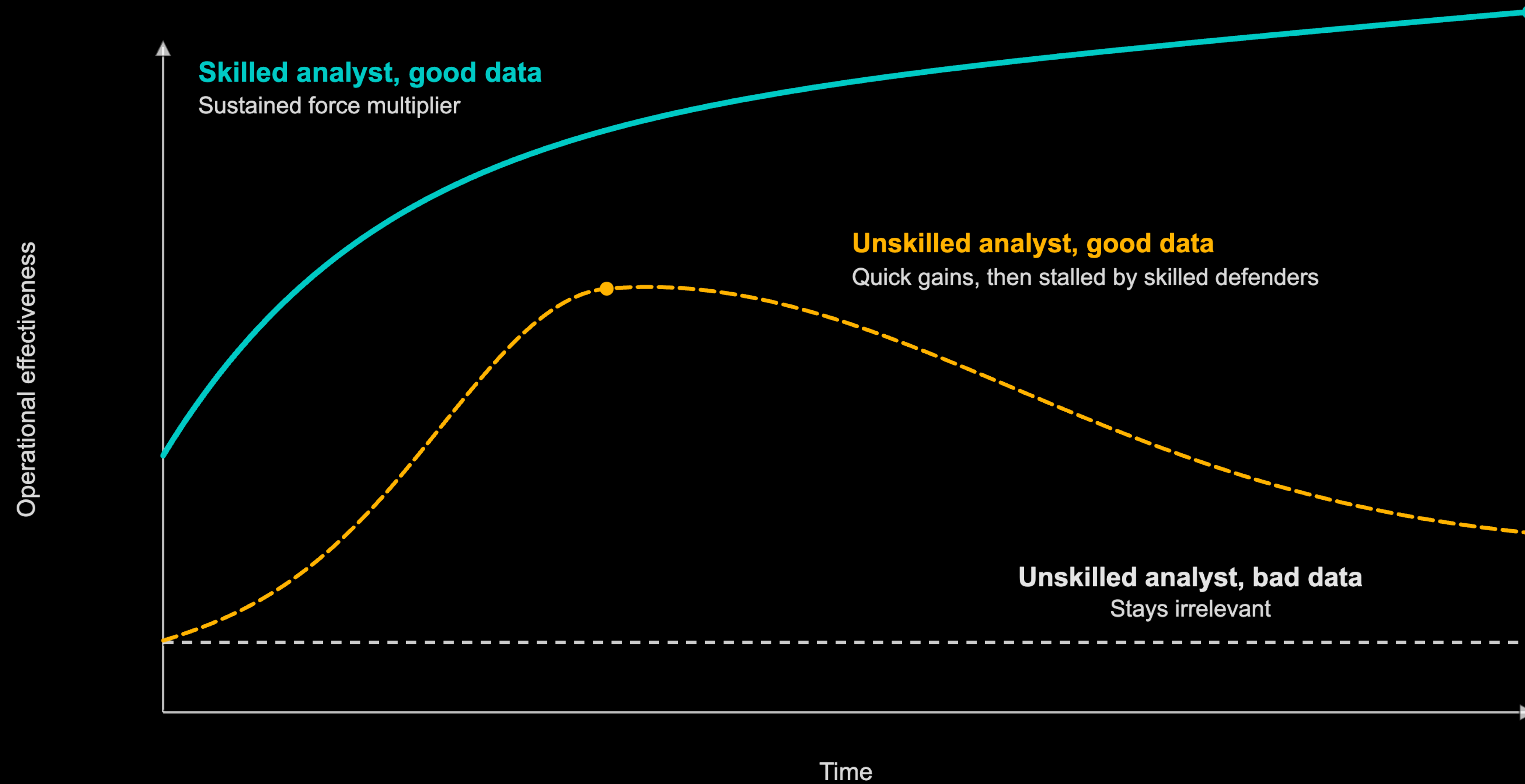
- PLC_Controller.exe (forces PLCs to STOP)
- PowerShell Modbus scripts
- Hacktivist C2 frameworks

Operational Intelligence

- Thousands of control tags stolen
- Process data exfiltrated
- Control loops mapped

The technical barrier between understanding ICS protocols and having working attack tools has collapsed

Adversaries Using AI





The Next Three Years



The Imperative: The Time To Act Is Now

THANK YOU

