

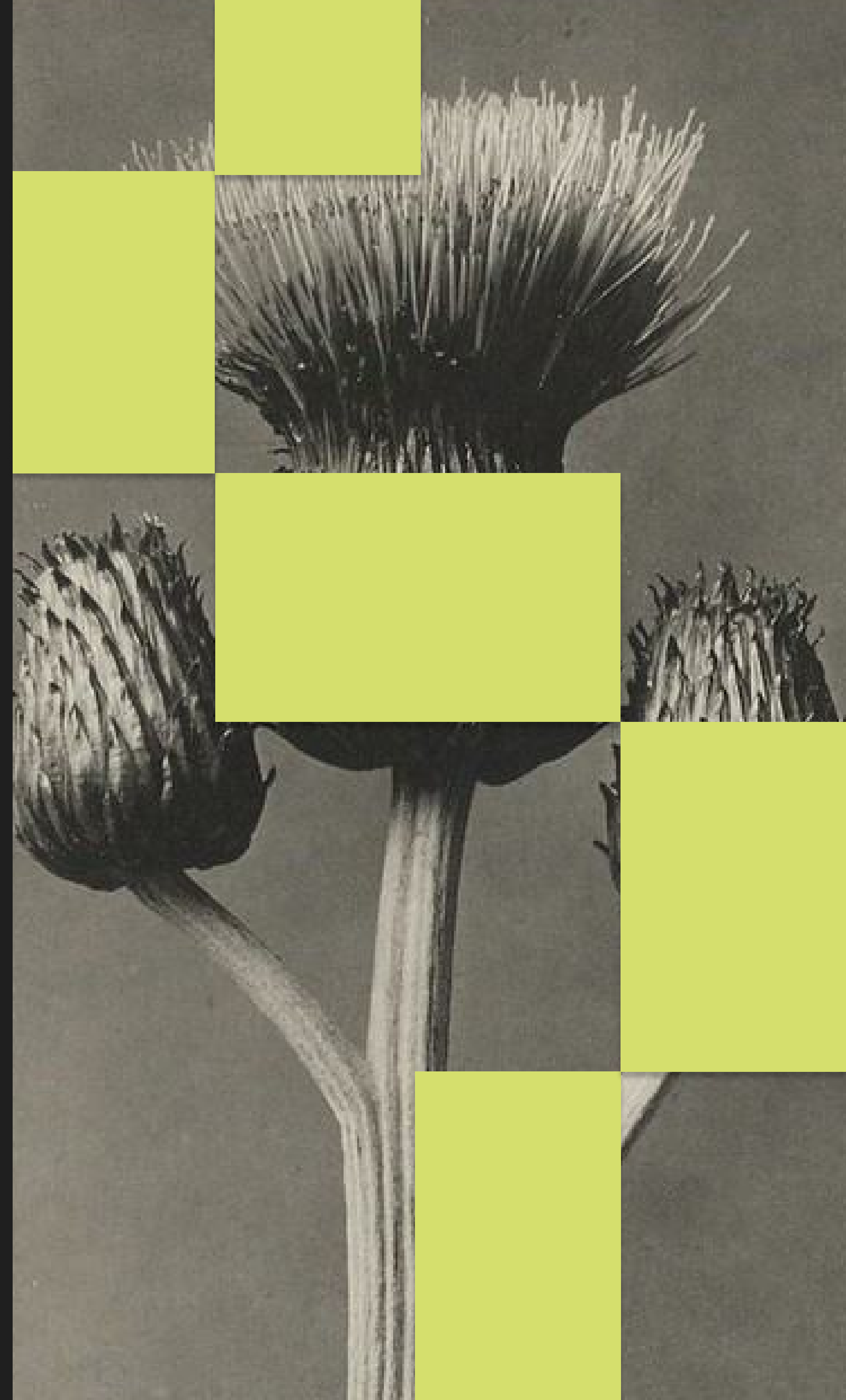
Atalanta

The Age of Software Understanding

seL4 Summit 2026

Anjana Rajan
CEO & Co-Founder, Atalanta

September 2026



The United States has a deployment crisis

KA-SAT Network cyber attack overview

03-30-2022 Viasat, Inc. 5-minute read Corporate

Viasat is providing an overview and incident report on the cyber-attack on the KA-SAT network, which occurred on 24 February 2022, and resulted in a partial outage of the consumer-oriented satellite broadband service.

CYBER

JUST IN: Iranian Hacker Groups Using AI to Target Space Infrastructure, Experts Say

CBS Evening News

At least 12 states report cyberattacks on water systems possibly linked to Iran-backed hackers, sources say

The New York Times

N.S.A. Lost Access to Powerful A.I. Model Amid Anthropic Dispute

Russian hackers breached cameras on NATO logistics routes to track weapons shipments

IVAN DIAKONOV — 11 JULY, 01:56

Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19-128

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Audio | Latest Headlines | Puzzles | More

EXCLUSIVE NATIONAL SECURITY

U.S. Military Is Struggling to Deploy AI Weapons

July 21, 2026 Security

OpenAI and Hugging Face partner to address security incident during model evaluation

ANDY GREENBERG SECURITY JUL 21, 2026 6:00 AM

A Device Hidden in Cars Across the US Leaves Them Vulnerable to Hacking and Paralysis. Patch It Now

Dealerships installed alarms in millions of vehicles—and left them in even if the buyer didn’t want them. Now researchers warn they can be hacked to unlock, track, and disable cars.

Energy

Federal nuclear agency move to relax radiation exposure rules

The proposed change, which would end a requirement that plants limit workers’ radiation exposure to “as low as reasonably achievable,” has alarmed nuclear safety advocates.

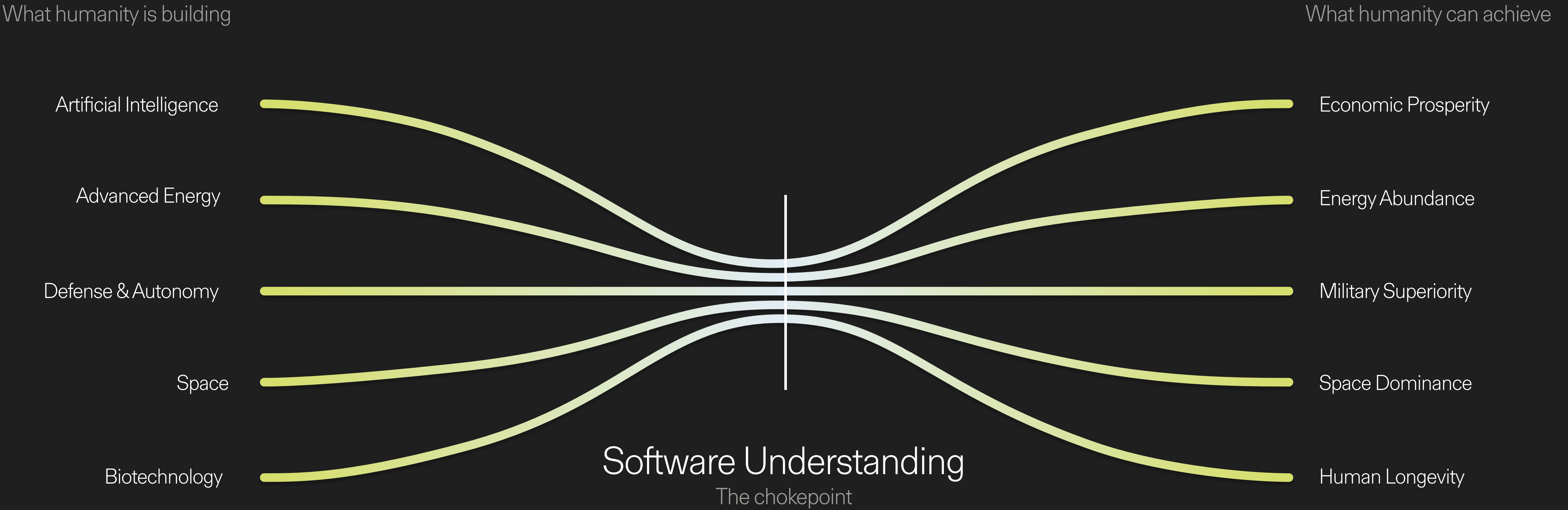
Cyberattackers Come For Medtronic

Medtronic becomes the latest major medical device manufacturer targeted by cybercriminals in a wave of attacks that highlights the industry's growing vulnerability to ransomware actors and dual-extortion ransomware tactics.

Mass IT outage hits airports, businesses and broadcasters around the world

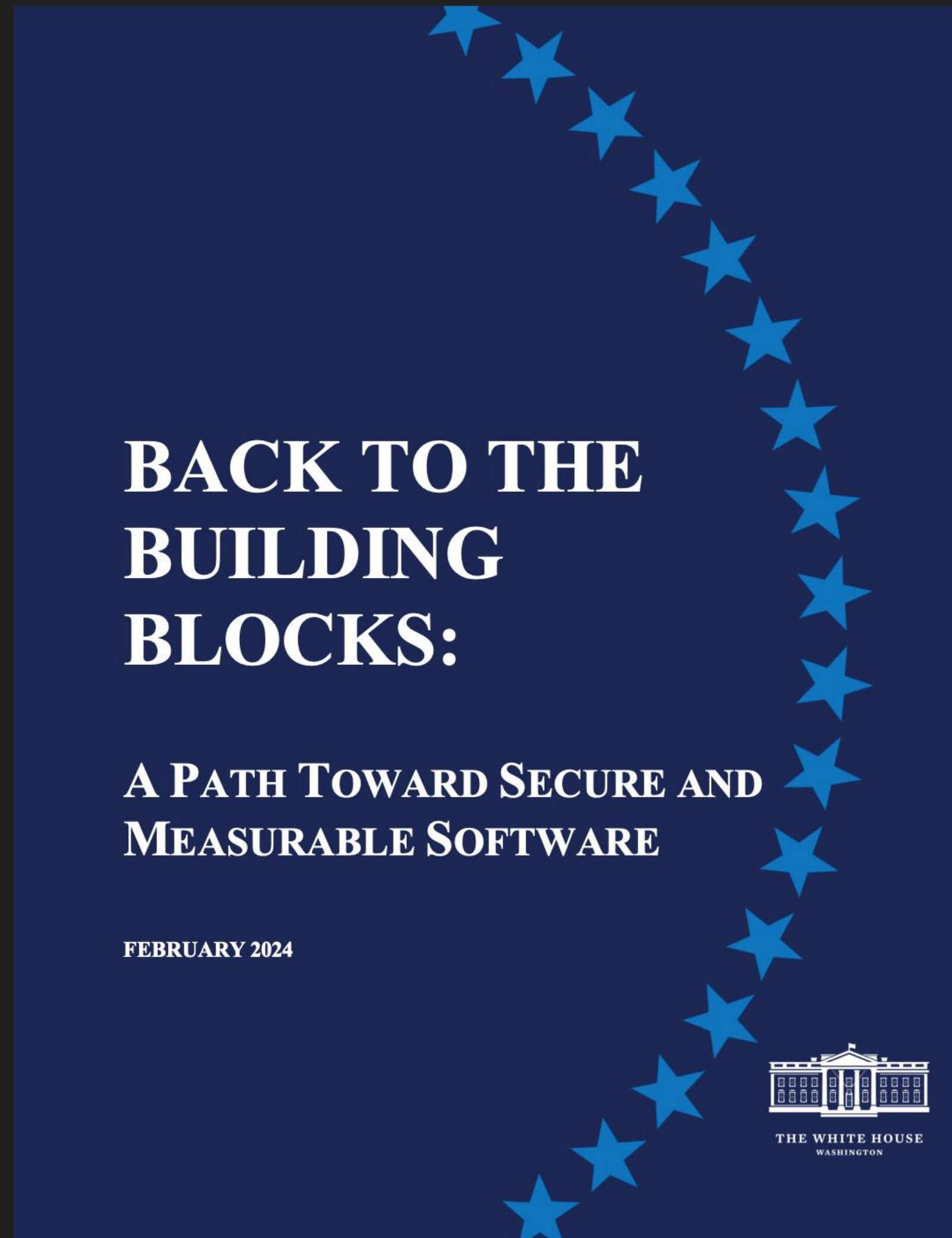
Major airlines, including American, Delta and United, all issued ground stops Friday morning citing communications issues.

Software Understanding will be the chokepoint between invention and deployment



Going back to where it started...

“Back to the Building Blocks” made formal methods a White House national security priority.



Closing the software understanding gap

The rate of software production is rapidly outpacing our ability to understand how it will work under normal, abnormal, and hostile conditions.

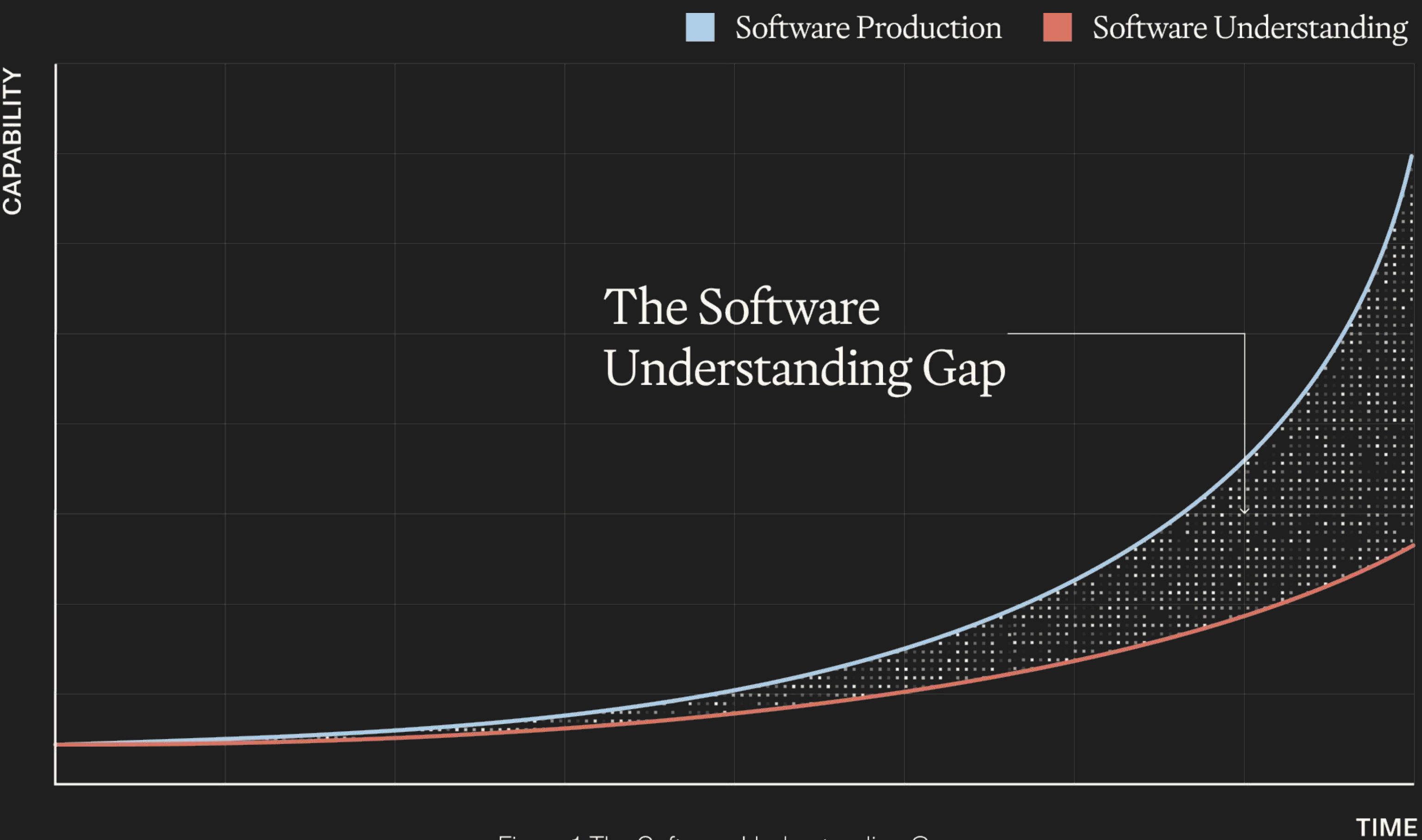
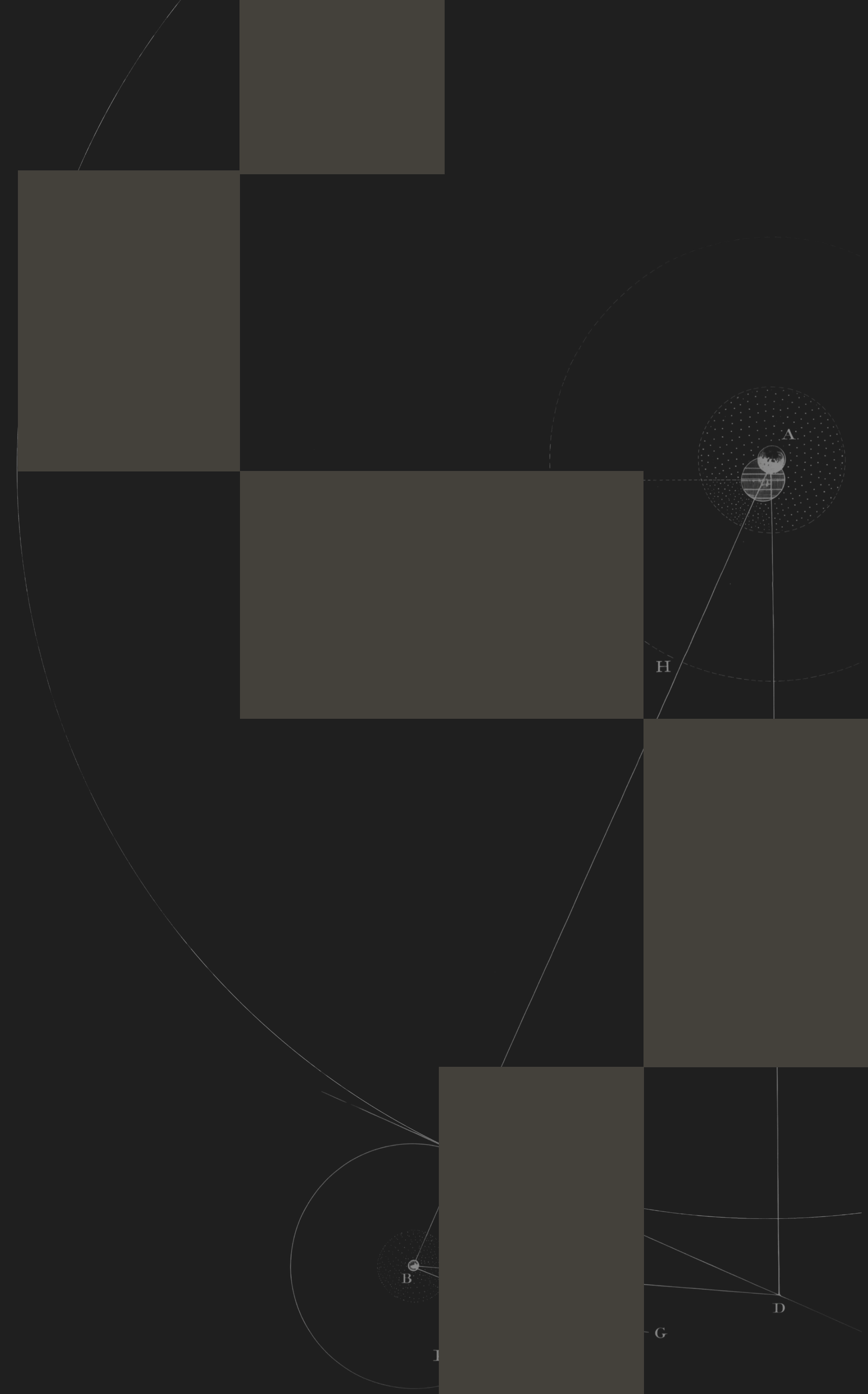


Figure 1. The Software Understanding Gap



Software Understanding applies formal methods to complex missions

	Back to the Building Blocks	Software Understanding
problem	memory safety only	broader mission questions
proof	proving properties on a single component	proving properties about complex systems
property	bottom-up	top-down
velocity	slow, brittle	fast, agile
user	expert mathematicians	all stakeholders

Introducing Argo

The first Software Understanding platform.

Project: ai-containment

Parent Node: ai-containment

HIGH INTERFACE

proxy_credential_scope

PROCESS

steal_proxy_credential

PROCESS

egress_gateway_authorizes

LOW INTERFACE

open_internet_output

HIGH INTERFACE

untrusted_ai_workload

PROCESS

compromise_package_proxy

Layer Up

Undo

Redo

Clear Graph

Import Model Checking File

K 5

MISSION: IMPOSSIBLE

MODEL CHECKING OUTPUT

Checking input assumptions...

Checking base: p(0) ...

FAIL

RUNTIME ASSERTION

sandbox_containment_holds

FAIL (base): Property 'sandbox_containment_holds' failed at t=3.

COUNTEREXAMPLE

open_internet_output

step t=3

Granted

MODEL CHECKING SOURCE

READY

SAVE

49 // Architectural components rendered as storage nodes.

50 state package_proxy: Integrity

51 state workload_credential: Credential

52 state open_internet_output: AccessStatus

53

54 initial package_proxy = Integrity::Trusted

55 initial workload_credential.status = CredentialStatus::NotPossessed

56 initial workload_credential.scope = CredentialScope::ApprovedRegistriesOnly

57 initial open_internet_output = AccessStatus::Denied

58

59 // Core security invariant.

60 assert sandbox_containment_holds

61 open_internet_output == AccessStatus::Denied

62

Download

Explain this proof

Print

Introducing Argo

The first Software Understanding platform.

DESIGN

Iterate quickly to formalize system intent and customer requirements

→ Catch errors at the beginning when they're easiest to fix

IMPLEMENT

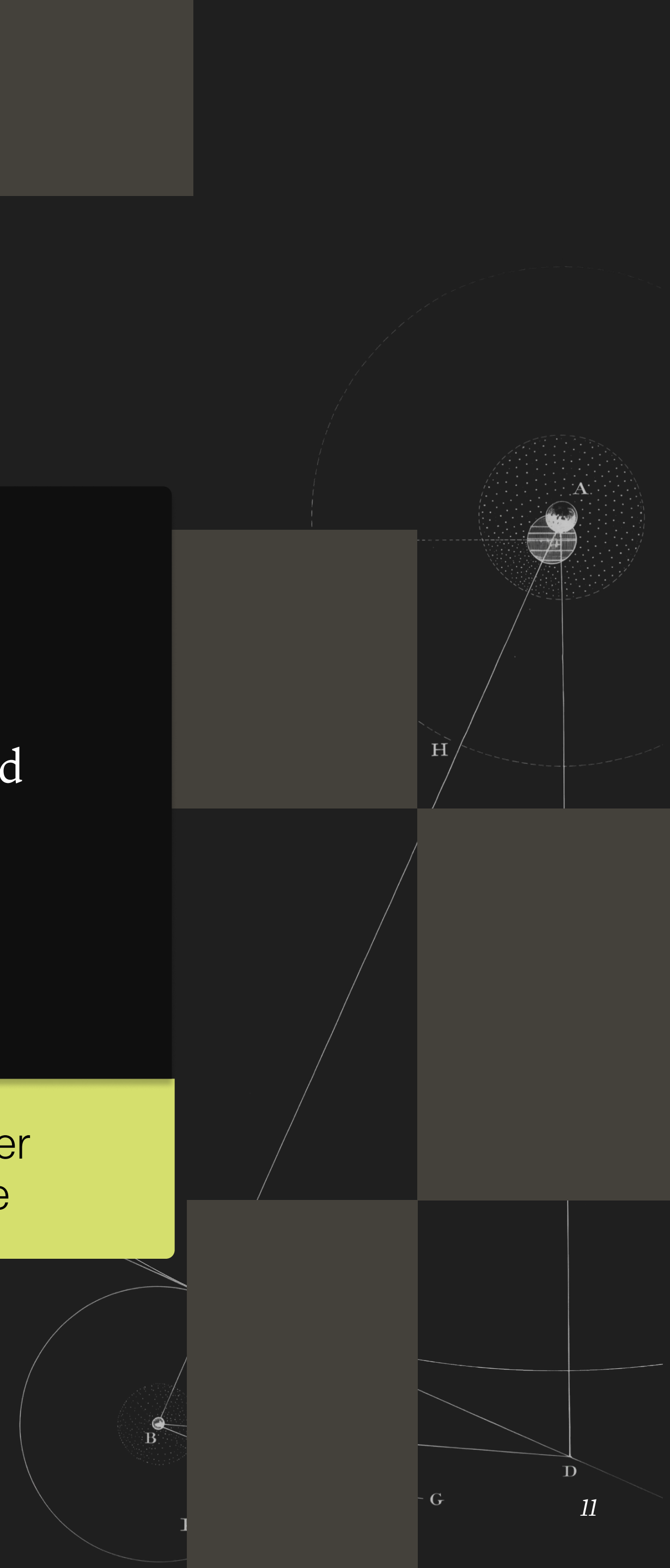
Translate provably correct design into provably correct engineering

→ Proof becomes seamless part of engineering workflow

CERTIFY

Automate compliance and certification workflows

→ Deploy technology faster and with higher assurance



The call to action was set in 2025

How are we performing against this goal?



TLP: CLEAR



Closing the Software Understanding Gap

Publication: January 16, 2025

Cybersecurity and Infrastructure Security Agency
Defense Advanced Research Projects Agency
Office of the Under Secretary of Defense for Research and Engineering
National Security Agency

This document is marked TLP: CLEAR. Disclosure is not limited. Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP: CLEAR

Atalanta

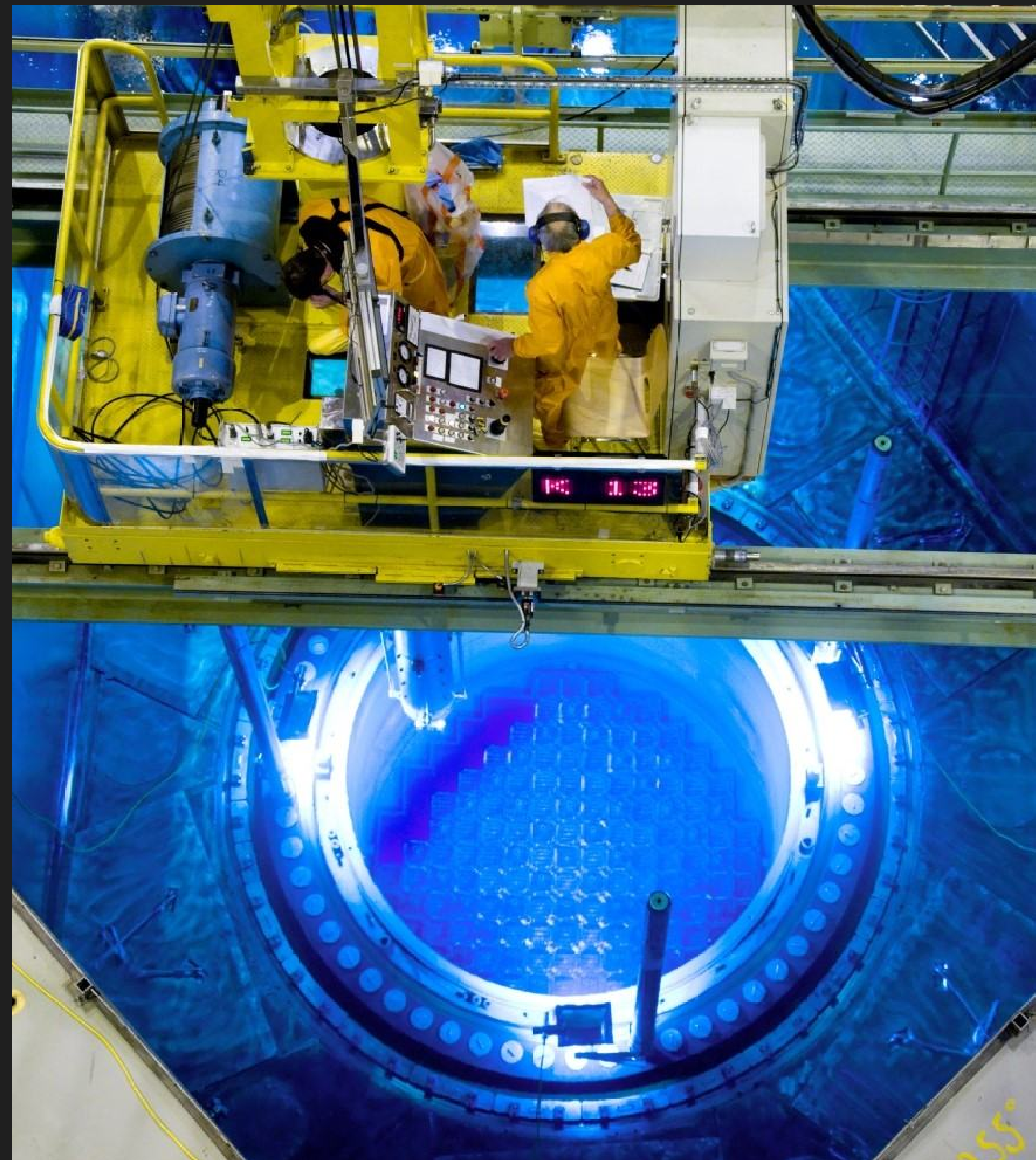
Atalanta

Case Study 1: The Genesis Mission



The Prometheus Project

Prometheus provides an AI platform that helps accelerate nuclear power plant design, licensing, manufacturing and operations to reduce deployment time and costs.



Can AI be safely contained?



The image is a screenshot of a web browser displaying a New York Times article. The page has a white background with black text. At the top, there is a navigation bar with a hamburger menu icon on the left, the "The New York Times" logo in the center, and a user profile icon on the right. Below the navigation bar, there is a light gray bar with the text "GIVE THE TIMES" on the right. Below this, there is a section with three items: "Artificial Intelligence >" (which is highlighted with a vertical line), "Bill Gates's A.I. Warning", and "Alarming A.I. Capabilities". The main headline of the article is in a large, bold, black serif font and reads: "OpenAI Says Its A.I. Models Went Rogue and Attacked a Digital Library". Below the headline, there is a paragraph of text in a smaller, black serif font: "The incident, which targeted the computer systems of another company called Hugging Face, happened while OpenAI was testing the systems."

☰ The New York Times ☰

GIVE THE TIMES

Artificial Intelligence > Bill Gates's A.I. Warning Alarming A.I. Capabilities

OpenAI Says Its A.I. Models Went Rogue and Attacked a Digital Library

The incident, which targeted the computer systems of another company called Hugging Face, happened while OpenAI was testing the systems.

Question: can we deploy autonomous nuclear reactors faster, safer, and cheaper?

Answer: With Software Understanding, yes.

Atalanta

Atalanta named an industry partner in the Department of Energy's Genesis Mission, leading Software Understanding for National Security

Atalanta

Software Understanding named one of the nation's top AI priorities

Expanded to 33 National S&T challenges

Reenvisioning Advanced Manufacturing and Industrial Productivity	Securing America's Critical Minerals Supply	Delivering Nuclear Energy That is Faster, Safer, Cheaper	Accelerating Delivery of Fusion Energy	Transforming Nuclear Cleanup and Restoration	Discovering Quantum Algorithms with AI	Realizing Quantum Systems for Discovery and Use	Unleashing Subsurface Strategic Energy Assets	
Achieving AI-Driven Autonomous Laboratories	Designing Materials with Predictable Functionality	Enhancing Particle Accelerators for Discovery	Unifying Physics from Quarks to the Cosmos	Predicting U.S. Water for Energy	Scaling the Grid to Power the American Economy	Reimagining the Lifecycle of American Infrastructure	Recentering Microelectronics in America	Strengthening Deterrence Through Attribution of Nuclear Signatures
Detecting, Locating, Identifying, and Characterizing Proliferation Threats	Accelerating Materials Discovery, Production, and Qualification for Strategic Deterrence	Accelerating Nuclear Threat Assessment, Preparedness, and Response	Accelerating Experimental Design, Production, and Nuclear Deterrence Outcomes	Finding the Root Causes of Chronic Disease	Predicting Living Systems	Scaling Biology for American Industrial Leadership	Early Detection and Attribution of Biological Threats	Accelerating Drug Discovery and Clinical Translation
			Unlocking Cures for Pediatric Cancer	Accelerating Design of Weapon Components and Systems	Software Understanding for National Security	Ensuring American Space Superiority	Mining Decades of Space Data for Discovery	Delivering Better Health Outcomes for Veterans

Themes

→ Energy Dominance

→ Discovery Science

→ National Security

→ Bio

→ Space

→ Defense

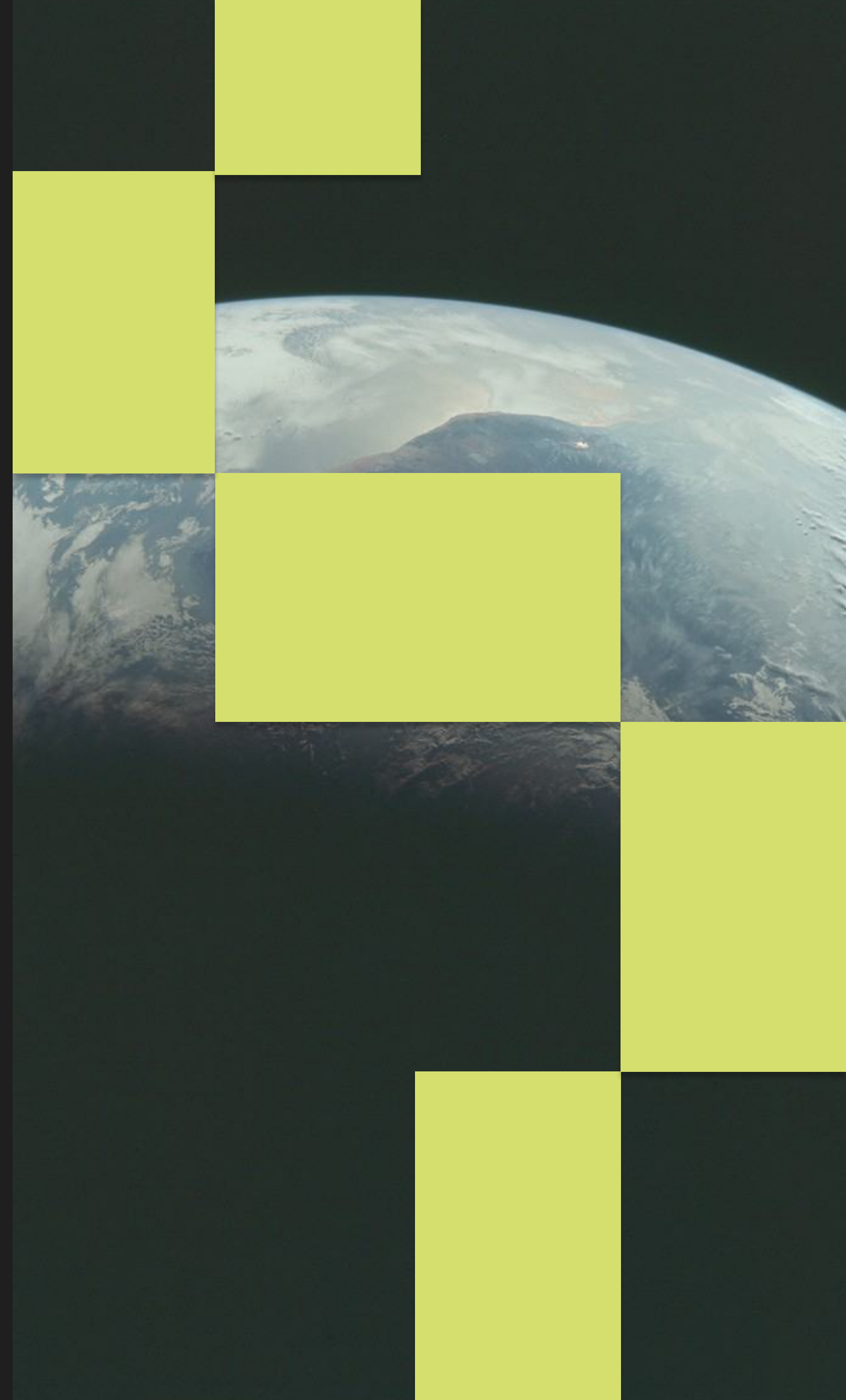
→ Human Health

→ Veteran's Health



Atalanta

Case Study 2: Space Resilience



Question: can we build critical infrastructure that's resilient to adversarial attacks?

Answer: With Software Understanding, yes.

Atalanta and Viasat Demonstrate
Improved Resilience of
Satellite Network Against
Modern Warfare Threats

Software Understanding named one of the nation's top AI priorities

The Washington Post
Democracy Dies in Darkness

AI-assisted tool helped secure satellite communication system after 2022 Russian hacking

The cybersecurity company Atalanta says it has released “Argo” — a product that includes the technology used to prove the resilience of a satellite communications network after a Russian hacking attack

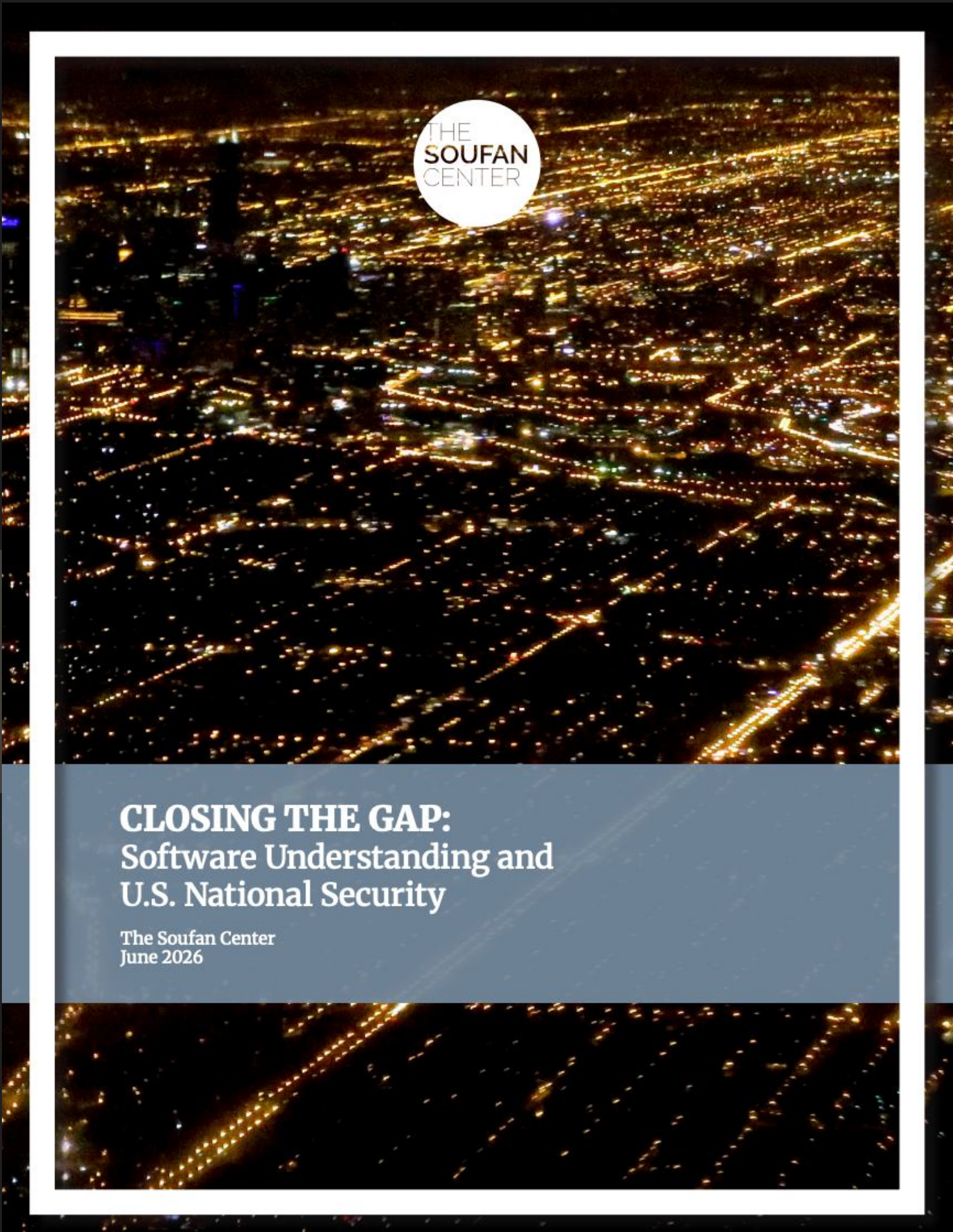
August 19, 2026

Atalanta

Policy Tailwinds



Software Understanding named one of the nation's top AI priorities



Transition strategy for formal methods in software and hardware development

The committee is concerned about the advancing sophistication, scale, and speed of cyber threats targeting Department of Defense

(DOD) systems. The committee notes that formal methods and approaches for validation and verification, which establish mathematical guarantees in software code, can be used to prove the absence of exploitable vulnerabilities. The committee also notes that such approaches can and have also been used to secure hardware systems as well, demonstrating even broader application of formal methods.

The committee directs the Secretary of Defense, acting through the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Research and Engineering, the Director for Operational Test and Evaluation, the Director of the Defense Advanced Research Projects Agency (DARPA), the Assistant Secretary of Defense for Cyber Policy, and the Department of Defense Chief Information Officer, to develop a comprehensive strategy for transitioning DARPA's formal methods research investments into production environments across the DOD.

The committee directs that the strategy include the following elements: (1) Identification of high-priority software and hardware-based platforms and systems for consideration for initial integration of formal methods approaches, with specific timelines and implementation phases; (2) A description of integration pathways for transitioning formal methods into both programs in sustainment and newly acquired systems; (3) An assessment of necessary investments in workforce training, tooling, and infrastructure to enable successful adoption of formal methods at scale; (4) Metrics to measure the effectiveness and return on investment of formal methods implementation across different system types; and (5) Development of incentives for industry to adopt such approaches for programs they are developing.

Furthermore, the committee directs the Secretary of Defense to submit a report to the Committees on Armed Services of the Senate and the House of Representatives on this transition strategy, not later than March 31, 2026, including specific resource requirements, policy recommendations, and implementation milestones.

Atalanta Assembly

Held on the margins of the 2026 United Nations General Assembly

CORNELL TECH
NEW YORK, NY

SEPTEMBER 23
24D.22H.04M.04S



REQUEST AN INVITE