Global Race Condition | The Week That Was

Week Ending April 25, 2026

Signal over noise, for people others depend on.

America's AI Incoherence is Driving CISOs to China

1. THE WEEK’S VERDICT

America’s AI Incoherence is Driving CISOs to — China?

Many weeks, the most impactful development is a breach, often in some new way. We’ve seen a number of novel patterns so far in 2026, including a new focus on chokepoints, dependencies, and control planes.

This week is different. The big thing this week was a capability demonstration. An arXiv preprint described AgentFlow, a multi-agent harness using Claude Opus 4.6 and Kimi K2.5, discovering 10 previously unknown zero-day vulnerabilities in Google Chrome, including two Critical sandbox escapes.

Mozilla separately confirmed using Anthropic’s Mythos model to find 271 Firefox vulnerabilities in a single automated sweep. A third paper (LLMVD.js) validated 84% vulnerability confirmation rates for LLM-based detection in Node.js packages, versus less than 22% for traditional tools (Thursday brief, April 23).

The attack surface has expanded faster than defensive tooling can compensate:

- Mythos operates at a METR 50% Time Horizon of 40 hours, meaning it can sustain autonomous work equivalent to a full human work week on complex tasks.
- The NSA is reportedly using it despite broader government restrictions on Anthropic.

- No CISO is wondering whether adversary nations are running equivalent pipelines, because of course they are.

But YOU can't have it, unless you use Chinese AI. Or hack Anthropic. Or use an open source variant.

American models are simultaneously too dangerous to allow in the US military supply chain, classified as critical to the US government, too dangerous to be widely exposed, and being hacked by doing script kiddie things like guessing the path to the model.

We all know adversaries are using this level of tooling to harvest as many zero days as possible. Weaponization is coming, at scale.

So the question of the day is whether your organization is auditing its own code at the same speed it is being audited by others. Since you probably don't have commercial access to the latest and greatest, the only quick path is to build it.

With Chinese models. DeepSeek V4 dropped this week.

Chinese AI models you can't see inside, by the way. Black boxes. Models called "open source", but you don't actually get the source code, or the training data. Only weights.

Take a look at that 27B parameter model and tell me where the malicious .csv values are. We've done a lot of research on data poisoning and neural trojans, and in our view it is naive to come to any conclusion other than that all major AI models are being actively manipulated by their nation state.

We know American models used for Federal sourcing are not allowed to discuss political issues like DEI or climate change, and Chinese models are not allowed to stray from 'core socialist principles' or discuss controversial topics like the reunification of Taiwan or the violence in Tiananmen Square in 1989.

What else is inside these models? You're not allowed to know.

To us, this looks like America stepping into a trap set by China. Summing it up:

Our incoherence from a policy perspective is driving American Defenders to Chinese models in order to defend against the American technology that is simultaneously poorly secured and too dangerous to release. Both OpenAI and Anthropic have been hacked multiple times; at least 3 times in the last month.

With everything else in the world going on right now, technology leaders' #1 priority should absolutely NOT be "Magic AI Money".

You need to be focused on Technology Debt.

You are on the clock, and you are behind. Weaponized AI is coming, and coming soon, it is not well-controlled, and your security teams are not prepared.

Anthropic's attempts to restrict Mythos-level capabilities have already failed, and we are all hovering like Wile E Coyote who just ran off the cliff, just before he falls.

The median hand-off time between initial access and secondary actor activity is now 22 seconds.

To make the tech debt problems worse, new AI tools with production environment access are now emerging as a new primary attack surface. The Vercel breach this week was an example of the above-mentioned pattern, but even that should take a back seat to Technology Debt.

Watch this space, and it won't take long. A wave of AI-enabled attacks are coming at machine speed.

Your technology debt is about to come due, with penalties and interest.

What our daily briefs got right: Tuesday identified the AI vulnerability discovery arms race as a top story and connected it to the Vercel supply chain pattern. Thursday confirmed the pattern with the function hijacking and cross-session attack research. The escalation from "research curiosity" to "production capability" was tracked correctly across the week.

What hindsight reveals: The briefs could have been more specific about the defensive asymmetry. Attackers can use open-weight models (DeepSeek V4, released Friday at 1.6 trillion parameters) without any usage restrictions. Defenders must operate within organizational policy, legal constraints, and procurement cycles. The gap between offensive and defensive adoption speed is the actual risk, and it was underweighted.

The Hormuz Stalemate Institutionalized

Iran began collecting tolls on Strait of Hormuz passage and deposited the first revenue into the Central Bank on Wednesday (Thursday brief, April 23). The

IRGC simultaneously seized two European-flagged vessels and attacked a third. A Pentagon assessment puts mine clearance at six months minimum. Oil topped $106 per barrel while the EU Commissioner for Economy confirmed $584 million per day in European economic damage.

This was the week the Hormuz crisis transitioned from a military standoff to an institutional revenue mechanism, and that matters for enterprise risk management and planning.

A military blockade can be resolved by a ceasefire. An institutionalized toll system creates a new baseline that negotiations must address. Iran is no longer asking to reopen the strait. It is negotiating the terms under which it will permit transit, a fundamentally different starting position.

The IRGC veto over civilian negotiators, identified as the central structural obstacle in Tuesday's brief and reinforced every subsequent day, hardened this further. IRGC Commander Vahidi publicly contradicted Foreign Minister Araghchi's announcement to reopen Hormuz. The heads of all three branches of government published synchronized loyalty oaths denying factional division. Leaders who are genuinely unified don't need to publish simultaneous statements saying so (Friday brief, April 24).

What our daily briefs got right: Our midweek assessment correctly predicted that the ceasefire would not produce a clean resolution. The IRGC veto was identified early and consistently reinforced with new evidence each day.

What hindsight reveals: The briefs consistently framed the IRGC veto as a problem to be solved. The contrarian view, that Iran's "fractured leadership" coexists with institutional coherence sufficient to sustain military operations, deserved more prominence earlier in the week. Hassan Ahmadian's pushback in Drop Site on Thursday ("Name another system whose top echelon are assassinated and is capable of continuing, and also waging, a retaliatory war effort") was the strongest challenge to the dominant analytical frame.

The CISA Budget Cut Creates a Coordination Vacuum During Peak Threat Activity

Cybersecurity takes spot 1 and 3 in this week's roundup, which should tell you something about the scale of the issues we're all facing.

The Trump administration's FY2027 budget proposes cutting CISA by $707 million, dropping it to just over $2 billion, while requesting $1.5 trillion in total defense spending (Friday brief, April 24).

The Stakeholder Engagement Division, which coordinates cyber defense with state, local, and private-sector operators, is among the shuttered programs. If it were a nation, cybercrime would be the third largest economy in the world, behind only the US and China, at around $10T. China-nexus intrusions increased 150% year-over-year per CrowdStrike.

Just as market forces and an incoherent US AI strategy pushes Defenders TOWARDS Chinese models.

The timing couldn't be worse; NIST is now limiting vulnerability enrichment as the CVE backlog grows. Mean time-to-exploit is -7 days (exploitation begins before patch availability on average, per Mandiant M-Trends 2026).

The infrastructure for vulnerability tracking is degrading at the exact moment vibe-coded AI tools expand the attack surface, while AI-assisted discovery has made vulnerability discovery too cheap to meter, breaking the white-hat / bug bounty market.

Even FDD, which almost always supports increased defense spending regardless of administration, publicly criticized these cuts. When a hawkish establishment think tank breaks with a Republican defense budget, the divergence is analytically significant (we covered this in our Friday brief convergence map).

Sphere of control implication: Organizations that relied on CISA coordination for threat intelligence, particularly water utilities, hospitals, and energy providers in your supply chain, will need to acquire equivalent intelligence commercially. Budget owners should expect vendor cost increases.

SLED (State, Local, and Education) and small to medium size enterprises, the Federal government isn't coming to help you, but there may be some government talent coming onto the market, if you can afford it. They're good people, and you should hire them.

US Munitions Depletion Now Constrains China Deterrence

CSIS confirmed the US has consumed at least 45% of Patriot interceptors, 53% of THAAD interceptors (possibly 80%), and 45% of Precision Strike Missiles in the Iran war (Thursday brief, April 23).

The report states prewar inventories were “already insufficient” for a peer competitor conflict. The Pentagon is approaching GM, Ford, and Oshkosh about manufacturing weapons. The Korean War production surge, the closest historical precedent, took 18-24 months to materially affect battlefield supply.

Taiwan signed six arms deals totaling $6.6 billion this week and an exercise called “Balikatan” proceeded with 10,000 US personnel and Japan’s first active participation.

The Pacific deterrence posture continues on paper while the inventory those forces would need is being consumed in the Middle East. Zelenskyy confirmed that a prolonged Iran war directly threatens US missile defense supply to Ukraine. The consumption is now documented by a primary CSIS report and confirmed by multiple independent analytical traditions, realist and interventionist alike.

Asian partners and companies relying on the US security umbrella for stability should factor these developments into their contingency planning. Regardless of the promises on paper, without US ability to deliver, your Plan B may become Plan A. Make sure Plan B is solid.

The Quantum Readiness Gap Widened on Both Ends

Google will complete its post-quantum cryptography transition by 2029, as will Cloudflare. US Federal agencies are not expected to complete the same transition until 2035.

IonQ published a “walking cat” blueprint describing fault-tolerant architecture that could run millions of logical operations using as few as 2,514 physical qubits, all on hardware already demonstrated in labs.

Quantinuum filed a confidential S-1 for an IPO at a rumored valuation above $20 billion. A 15-bit ECC key was broken on quantum hardware, winning the Q-Day Prize. Cisco announced a prototype universal quantum switch routing quantum information at room temperature over existing telecom fiber with less than 4% signal degradation.

The commercialization timeline compressed this week: hardware capability moved forward while government policy remained static.

The EU Cyber Resilience Act requires products expected to remain in use past 2030 to have upgradable encryption, with full effect in December 2027. The US has no equivalent requirement.

Enterprises selling to both markets will build to EU standards by default. That is the correct outcome, happening through regulatory arbitrage rather than US leadership.

---

2. TREND TRAJECTORIES

AI-assisted code auditing as standard practice: ACCELERATING. Confidence: high. What would change the assessment: evidence that AI-assisted discovery produces unacceptable false positive rates in production (no such evidence has emerged).

However, what we do know from the field is that AIs often do not understand the full context of what “Production” means, and most organizations struggle with keeping lower environments and production in synch. This is going to matter a LOT when it comes to trying to work out what issues are real and which ones are incomplete or mistakes.

It won’t be long until developers are using AI to reject AI ‘false positives’ back to security teams, who will ask AI who’s correct.

Neither will understand the findings, and cybersecurity insurers will deny claims based on this analysis. This isn’t going to be fun for anyone.

Third-party AI tool supply chain compromise: ACCELERATING. Vercel/ Context.ai was confirmed and the template is now a trend:

infostealer hits AI tool vendor, OAuth token becomes beachhead.

Function hijacking attacks are achieving 70-100% success rates against agentic AI systems and cross-session attacks are evading all session-bound detectors, representing the next evolution.

Direction: accelerating. Confidence: high. What would change: vendor adoption of hardware-bound tokens and mandatory MFA for all AI tool OAuth grants, neither of which is happening at scale.

Iran Hormuz institutionalization: ACCELERATING. Busy week; the transition from military tactic to institutional revenue mechanism took four days.

Direction: accelerating toward permanence. Confidence: high. What would change: a unified Iranian negotiating position that includes reopening terms. The IRGC veto makes this unlikely in the near term.

NATO cohesion: DECELERATING. Pentagon email floating Spain's suspension. EU leaders requesting Article 42.7 mutual assistance blueprint. Europe approving 90 billion euro Ukraine loan independent of US.

The trajectory is not collapse but controlled divergence. Direction: decelerating cohesion, accelerating European institutional independence. Confidence: medium. What would change: a dramatic external threat (Chinese military action in the Pacific) that forces alliance re-consolidation.

US cyber institutional capacity: DECELERATING. CISA budget cut, NIST vulnerability enrichment degradation, Cybercom 2.0 not reaching full operational capability until 2031, only one of 13 Cyber Command general officers with a cyber background.

Direction: sustained decline. Confidence: high based on documentary evidence (budget proposals, organizational assessments). What would change: congressional restoration of CISA funding, which has historical bipartisan precedent. Without restoration and funding, "We are NOT from the government, and we are NOT here to help". Employers should snatch up this talent; you're going to need it.

Quantum commercialization timeline: ACCELERATING. IonQ blueprint, Quantinuum IPO, Cisco quantum switch prototype, Q-Day Prize ECC key break, Pennsylvania Keystone AI+Quantum Factory, regional quantum ecosystems forming faster than federal policy.

Direction: strongly accelerating. Confidence: high. What would change: a fundamental physics barrier discovered in scaling fault-tolerant architectures. No such barrier has been identified.

---

3. HOW WE CALLED IT

CORRECT CALLS

IRGC veto as the central structural obstacle to negotiations. Called in Tuesday's brief (April 21), reinforced every subsequent day, confirmed by ISW's April 23 special report documenting Vahidi's specific actions to block Araghchi and Ghalibaf.

Hormuz selective-access regime evolving into institutional revenue. Called in the April 8 midweek assessment ("watch for whether Iran establishes formal fee-based permitting"), confirmed by toll collection and Central Bank deposit on April 23.

US-Israel divergence sharpening. Called in the April 8 midweek scorecard, reinforced throughout the following weeks.

AI-assisted vulnerability discovery crossing the production threshold. Called in last Thursday's brief and immediately validated by three independent academic papers plus Mozilla's production deployment.

WRONG CALLS

Overconfidence in Iran's refusal to negotiate. The April 8 midweek assessment explicitly graded this as "CHALLENGED." The brief treated Iran's stated refusal of a temporary ceasefire as a high-confidence behavioral prediction rather than a negotiating position. The confidence level was too high. The lesson: when an actor says "never" under escalating existential pressure, discount "never" by the rate of escalation.

Underweighting Trump's escalation-to-deal pattern. The midweek assessment acknowledged this explicitly: the briefs did not model Trump's established negotiating pattern (threaten annihilation, then announce a deal) as a predictor of ceasefire timing.

BLIND SPOTS

DeepSeek V4's release was underweighted. The Friday brief covered it, but the briefing cycle did not adequately anticipate how the release of a 1.6-trillion-parameter open-weight model with domestic Chinese chip compatibility changes the export control calculus. The simultaneous threat CISOs face from offensive AI will drive otherwise hesitant CISOs to Chinese models, potentially embedding

Chinese black boxes in key security functions. We didn't pull all this together until late in the week.

The AI deskilling research was identified but not connected to enough domains. Thursday's brief connected it to the munitions production surge (workers trained with AI assistance may underperform when AI is unavailable).

SCORE: Mixed. Called 4 of 6 testable predictions correctly. The structural analysis was consistently sound. The confidence calibration on Iranian behavior was too high. The connection between DeepSeek V4 and the export control calculus was late.

---

4. ARTICLES WORTH READING IN FULL

Responsible Statecraft: Who is responsible when an AI weapon pulls the trigger? The best single piece this week on why AI targeting accountability is not a military ethics problem but a structural legal architecture failure arriving in commercial enterprise liability within 18 months. The mechanism it describes (deep learning outputs that cannot be reverse-engineered) is identical to the accountability gap facing enterprise AI deployments.

War on the Rocks: Resilience Without Capacity: The Fatal Flaw in America's New Cyber Strategy The most direct analytical treatment available of the contradiction between the White House's ambitious cyber strategy and the workforce cuts gutting it. Essential reading for any board briefing on federal cybersecurity posture.

FDD: Why the government must accelerate quantum preparedness now Compares Google's 2029 PQC transition deadline against federal agencies' 2035 target, with specific attention to critical infrastructure control systems that cannot be updated via software patch. The argument you make to your board if you are responsible for OT/ICS security.

War on the Rocks: The United States Is Repeating Its Silicon Mistake with Gallium Nitride Zero US strategic reserves when China's export ban landed. The specific mechanism by which the US ceded gallium dominance follows the exact pattern it followed with silicon. If your products touch radar, EV power electronics, 5G, or advanced power supplies, you have exposure.

War on the Rocks: I'm Sorry, Dave. I'm Afraid I Can't De-escalate: On (AI) Wargaming and Nuclear War 95% nuclear signaling rates across 21

frontier model match-ups. This is a specific, citable finding that will define the AI-in-national-security debate for months. Read the methodology before someone asks you about it.

Responsible Statecraft: Catholics finally splitting with Trump over Iran war and Israel The best piece this week on how the Evangelical-Catholic coalition fracture tracks toward November midterms, with specific poll numbers, named individuals, and the theological arguments each side is actually making. Essential for understanding the domestic political constraints on US Iran war policy.

FDD: Finish the job: Why a half war with Iran is the most dangerous outcome The strongest available articulation of the achievable-objectives case, including the detail that Pickaxe Mountain may soon be beyond reach of the most powerful US and Israeli ordnance. Essential counterweight to the anti-interventionist consensus in the source pool.

---

5. NOW WHAT: ADVISORY ACTIONS (WEEKLY)

We recommend actions based on expanding concentric circles, starting with the innermost ‘sphere of control’, expanding to ‘sphere of influence’, then ‘sphere of interest’.

SPHERE OF CONTROL (do this Monday)

1) **Audit AI tool OAuth grants.**

The Vercel/Context.ai breach pattern was confirmed three times this week. Every AI coding assistant, design tool, and workflow automation with production environment access is a potential prior-compromise vector.

- Document which AI tools have OAuth access to which environments.
- Revoke any that are not actively justified.
- Add this to your quarterly vendor review.

The attack chain is infostealer hits vendor, OAuth token becomes beachhead, 22-second hand-off to secondary actor.

2) **Begin AI-assisted code auditing on critical systems.**

Organizations not running this type of sweep are being audited by adversaries with equivalent or better tools. If your security team has no policy on AI-assisted vulnerability research, that gap is the Monday conversation.

How you do this while managing the risk of Chinese AI tooling in your organization; THAT'S the conundrum we help our clients with, and it is a tough one. CISOs everywhere are in a tough spot, but not all realize the degree just yet.

3) **Rotate secrets for Vercel and any AI tool integration added in the last 90 days.**

This should be obvious; if your CI/CD pipeline touches Context.ai or Vercel, the secrets may be compromised.

4) **Patch Cisco SD-WAN (CVE-2026-20133).**

Federal deadline was Friday. If you have Cisco SD-WAN in your environment and have not patched, do it Monday morning.

SPHERE OF INFLUENCE (start this conversation)

1) **CISOs: Request cloud provider continuity plans for Gulf cable disruption.**

If you have workloads in Middle East cloud regions or financial clearing through UAE-connected institutions, request failover documentation.

IRGC-linked media explicitly threatened cable infrastructure this week.

Ask vendors: what is the latency impact of rerouting through European or Asia-Pacific nodes?

KEY: Ask your vendors BEFORE your auditors or Board members ask it of you.

2) **CIOs: Brief your board on the PQC migration gap.**

Google and Cloudflare complete by 2029. Federal agencies by 2035.

Begin your cryptographic dependency inventory. You are not going to be early for this.

3) **CISO / BCP: Raise the CISA coordination gap with your critical infrastructure vendors.**

Water utilities, energy providers, and healthcare operators in your supply chain have been receiving CISA early warning, but that pipeline is being cut. Ask your OT vendors what their threat intelligence plan is without CISA coordination.

Critical infra is called critical for a reason. Make sure you know where your org stands.

4) **CEO / Board: Ask your CFO or CRO to model Hormuz closure at 6 and 12 months.**

Energy costs are the obvious impact. The secondary molecular supply chain effects (fertilizer, polyethylene, industrial gases) hit 6-9 months after physical disruption and most financial models are not capturing them.

SPHERE OF INTEREST (understand this to make better decisions)

1) **The AI arms race is now bilateral and asymmetric.**

DeepSeek V4’s release as an open-weight model means offensive AI capability is freely available.

Defensive deployment requires procurement cycles, policy approvals, and organizational coordination.

The gap between offensive and defensive adoption speed is the largest single cybersecurity risk for the next 12-18 months.

Factor this into security architecture decisions and vendor evaluation. Favor tools that can be updated as rapidly as the threat landscape shifts.

Understand that both American and Chinese models may be backdoored by the nation state in question. Remember cost to exit, and that models are not immediately fungible / changeable without impact.

2) **European strategic autonomy is an investment thesis, not just a geopolitical observation.**

The EU is building defense procurement infrastructure, cyber coordination mechanisms, and industrial policy independent of US alliance commitments.

For enterprises operating in both markets, the regulatory and procurement environment is bifurcating. EU standards (Cyber Resilience Act, AI Act, Article 42.7 mutual assistance) will increasingly set the floor for global compliance.

3) **The Iran war's secondary supply chain effects are arriving on a 6-9 month lag.**

Oil is an input into almost everything, and the disruption isn't limited to oil. Fertilizer, bromium, helium, ammonia, ethylene, urea, DRAM pricing, and hydrogen disruptions are just a few of the others.

If your supply chain touches any of these inputs, the disruption will manifest in Q3-Q4 2026, not today.

---

6. METADATA

- **Days covered:** April 21–24, 2026 (Tuesday, Thursday, Friday briefs; April 8 midweek assessment for prediction tracking)
- **Total unique sources analyzed:** 561 across the week's briefs
- **Domains active:** Cybersecurity, AI & Technology, Quantum Computing, Geopolitics & Geoeconomics (Iran/Hormuz, Middle East, NATO/Europe, Western Hemisphere, China-US, Russia-Ukraine, Turkey-Israel, Libya, Mexico, Taiwan, Horn of Africa), Consciousness & Human Behavior, Eschatological/Religious, Macro/Finance
- **Analytical confidence:** High signal week. The Iran-Hormuz structural analysis achieved rare cross-source convergence (ISW, FDD, Drop Site, Al-Monitor, Haaretz, Responsible Statecraft all confirming the same structural dynamics from incompatible analytical traditions). The AI vulnerability discovery acceleration was validated by independent academic research plus production deployment. The munitions depletion assessment rests on a primary CSIS report. The quantum readiness gap is documented from both private sector and government timelines. The CISA budget story has a documentary evidence base. Primary analytical gaps: limited sourcing on Chinese domestic political dynamics, limited India/ASEAN coverage despite Pacific developments, no direct Iranian civilian sources beyond Iran Dispatches.
- **Lenses activated this week:** All overlays (Dugin, Technate, Greene, Eschatological, Realist/Economic). All six theaters were represented. Mirror test applied to NATO fracture and Hormuz stalemate. Faction analysis applied to Iran (IRGC vs. Civilian), Israel (secular-Tel Aviv vs. Religious-Jerusalem vs. Greater Israel), and US (military-industrial vs. MAGA-Technocratic vs. Mainstream financial).

Subscribe: globalracecondition.substack.com | Watch: YouTube @globalracecondition | Know someone who should be reading this? Share the link.
