OVERHAUL

CARGO CRIME SERIES

#2 NOV 2025

THE ATTRACTION OF AI INFRASTRUCTURE

THE NEW GOLDRUSH AND THE MODERN OUTLAW

THE ATTRACTION OF AI INFRASTRUCTURE

THE NEW GOLDRUSH AND THE MODERN OUTLAW

For those outside of the industry, AI is often thought about in the abstract. Little consideration is given to the physical components; servers, GPU's (graphics processing units), specialised chips, racks, networking, cooling, and power supply systems; the body if you like; the flesh and bones of sentient beings in the shadows, there to answer questions and to optimise the world.

THERE'S SOMETHING ELSE IN THE SHADOWS TOO. SOMETHING WATCHING...

Observing high value, high risk, high consequence infrastructure being produced, moved, integrated and operated. Something spying the industry, monitoring a multitude of hands who move portable, expensive, (and in the wrong hands, dangerous) components globally.

Change has come, rapidly, making entrepreneurs and financiers shift the direction of investment.[1] **The AI Gold Rush has begun.** CPU investments are now dominated by AI servers, the spend doubled by hyperscalers (to the tune of US $202 billion), and forecast to be operating US $1trillion in AI server assets in the next couple of years.[2]

As outlined in our previous paper, **'Inside the Billion Dollar Black Market of Stolen Supply Chains,'** we have seen illicit enterprise groups operate in the shadows, organising and planning. They are highly sophisticated and well-structured organisations, maximising profits while minimising risk with a network of 'specialists' within their ranks. As the Modern Outlaw, they follow profit, power and the leverage of influence. AI infrastructure, strategically and financially, is their gold; low risk set against high reward. They are in the shadows and they are mobilising.

1. Greenstein, Shane. 'The AI Gold Rush'. IEEE Micro 43, no. 6 (2023): 126–28. https://doi.org/10.1109/MM.2023.3322049.
2. Gartner Forecasts US$202bn Spend on AI Servers in 2025 | Data Centre Magazine

Many organisations have invested heavily in cybersecurity for endpoints, networks and applications but the infrastructure for AI often falls between the cracks. The sheer scale of it coupled with rapid scaling means security and chain of custody is secondary to operational deployment. A critical fault line and one that has been seen by organised crime groups. This is the perfect storm and an international collaboration. High value and low detection, the perfect ingredients for exploitation. The theft isn't simply about the hardware. Cryptocurrency mining, algorithmic trading, and data harvesting all become feasible with stolen AI components.

CARGO THIEVES ARE SCALING RAPIDLY AND ARE BECOMING INCREASINGLY INNOVATIVE

Black market demand for AI servers and chips is exploding and with a price tag of about $3m per rack. Cargo thieves too are scaling rapidly and are becoming increasingly innovative, knowledgeable of the vulnerabilities in the chain of custody and well versed in geopolitical competition. The demand for data centres has boomed. Projects face massive challenges in coordinating people, resources and products right the way through from OEMS to staff onsite. Chain of custody, asset management problems, schedules, coordination, delivery and control of inventory all become weak points and cast longer and longer shadows. In addition to the bricks and mortar models of data centres, we are also seeing hybrid, private and mobile data centres.

Thought leaders and supply chain managers need to think about where the cracks are. **Every deployment of AI infrastructure needs critical evaluation.** What are the risks and what is the cost if this infrastructure is stolen? Each component is a high value asset. Management, monitoring and pre-empting the weak points through production, movement, integration and operation are crucial. Governments, industry leaders and security experts need to take a leaf out of the organised crime playbook and collaborate together to understand the threats, rapidly scaling their collective intelligence. Policy needs to reflect the seriousness and the international element to the organised and highly profitable crime of AI infrastructure theft.

Routes are becoming riskier and more AI infrastructure shipments over air and land are being targeted. Crime rates are going up due to the increased value of shipments and companies stockpiling. High value, high risk, and high consequence infrastructure a sitting duck in distribution centres. Since around 2022, the US export controls have tightened like a hangman's noose and relate to semiconductors, chipmaking tools and related technology that might assist China in advanced computing, AI or military applications. Certain Chinese companies or those related to trade in China are placed on the US Entity list, meaning US companies cannot export machinery, tools, advanced AI chips or any technology used for making advanced chips to them without a specific licence. This restriction extends beyond the US and includes products made abroad using US origin tech or software. The logic being that it closes loopholes. America's AI action plan has made end-to-end traceability for AI hardware a compliance mandate, meaning gaps in physical security, supply chain vulnerabilities, theft of hardware and insider risk, punishable and non-compliance (knowingly or not) with policy and legislation could lead to severe penalties.

THE INCENTIVE FOR ORGANISED CRIME NETWORKS TO TARGET AND STEAL THE CARGO HAS EXPLODED.

The same restrictions have fuelled the fire of black-market activity. The incentive for organised crime networks to target and steal the cargo has exploded. The Financial Times has reported that despite the ban, at least a billion dollars' worth of Nvidia b200s and other banned chips have been shipped to China. That's a billion dollars' worth between May and July of 2025. Three short months. They also reported **sellers can make more than $100,000 for the sale of a single rack with eight GPUs.** High value, high risk, high consequence. That's a lot of money to fund a multitude of other criminal enterprises. Chips are moved around through third countries or via false declarations to mask the final destination and false entities may claim end-user permissibility under a false licence. Insider jobs, smuggling and the laundering of stolen infrastructure through cross border networks is the tip of the iceberg when it comes to the skills of the organised crime groups globally. They have demand channels open and ready to receive the goods and corrupting goods, forging documents, hacking logistics and rerouting shipments is just another day's work in their shadowy office blocks. As we've outlined, they follow profit, power and the leverage of influence. AI infrastructure, strategically and financially, is their gold.

David Warrick, Executive Vice President of Overhaul, hasn't seen anything like this in three decades of working in supply chain. He said, ***'This isn't opportunistic theft. This is organised crime. It's mobs and cartels who have infiltrated the supply chains.'***

For AI Infrastructure to be secure, the chain of custody, shipment tracking, product tamper detection and every other stage of production, movement, integration and operation must be floodlit, transparent and foolproof. There can be no shadows and there can be no fault lines. Visibility, the eagle eye of secure custody, and traceability is the answer.

Recognising AI infrastructure as a high value, high risk, high consequence target, and not just the data or applications it enables, is crucial. Thought leaders, security architects, and policymakers must act proactively, because the shadowy groups eyeing this technology are already doing so. AI infrastructure isn't just portable components to be sold at a profit. In the wrong hands, it's a weapon, a profit engine, and a competitive advantage. The time to protect it is now. AI hardware is the new target and Overhaul is its defence. If it powers AI, they protect it, at the edge, on the move and on site.

Overhaul understand the global climate their clients are operating in and their networks, technology, and innovation, keeps them ahead of these illicit enterprises. Overhaul have the eagle eyed view and they are watching. They are a step ahead and are the leading supply chain visibility and risk management software solution turning real time visibility into actionable solutions for compliance, insurance and risk mitigation. Trusted by companies across industries, Overhaul supports global freight operations for major brands like Microsoft, Google, Apple and Dell.

With Overhaul's SaaS platform, organisations can monitor sensitive, high value shipments anytime, anywhere.

Advanced risk management tools help detect and prevent potential threats before they escalate. Overhaul collaborates with law enforcement to support cargo theft recovery and leverage insights from global intelligence partners to keep customers informed of emerging risks.
Visibility is the first line of defence in managing and securing the supply chain. For leaders who have asked the question, Is my AI Infrastructure secure?
Overhaul is the answer.

For a free demo or to speak with one of our representatives contact us at https://over-haul.com/request-a-demo/