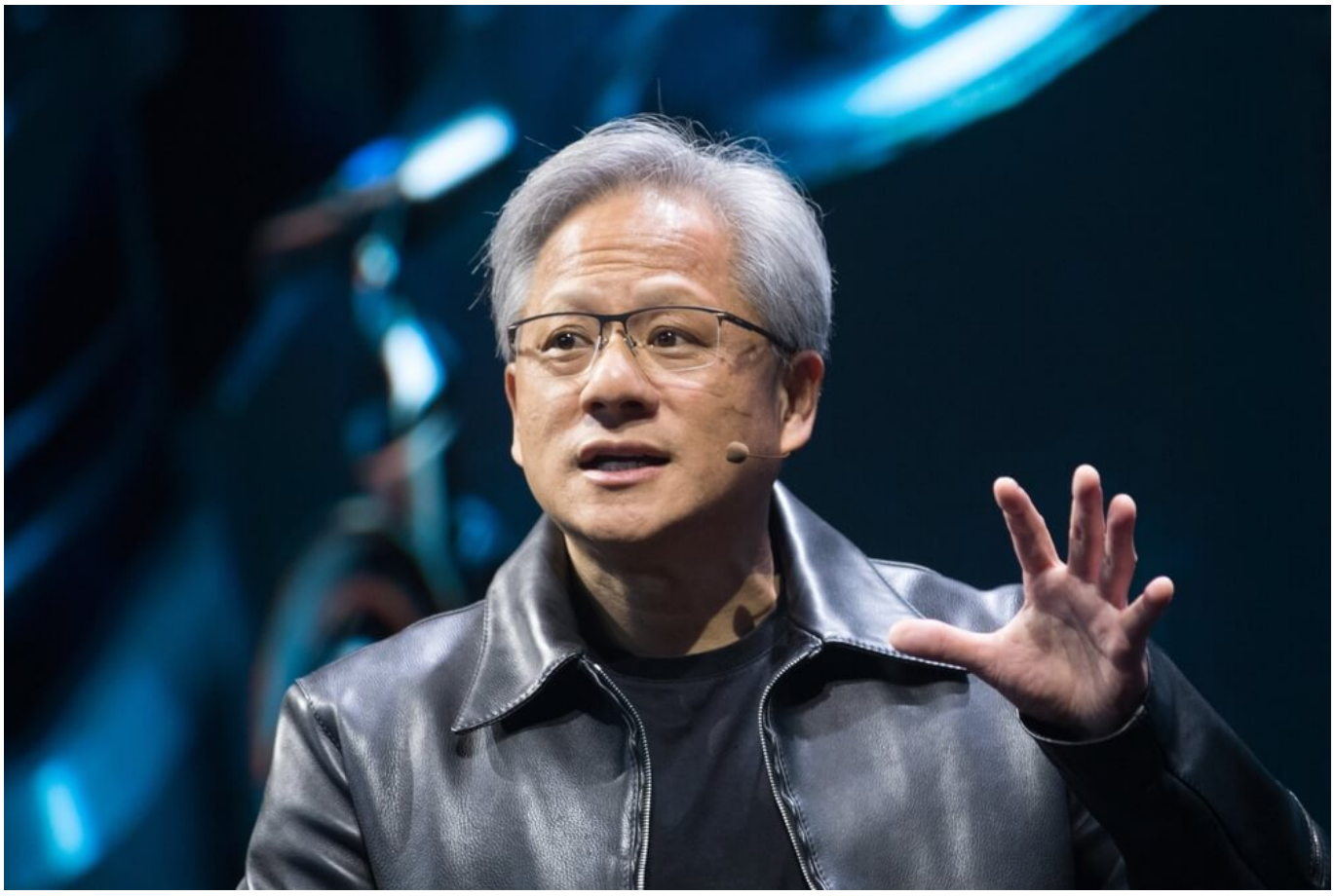
Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Sean Wiswesser

China won the Nvidia spy scandal – without recruiting a single American spy



Jensen Huang's resignation as CEO of Nvidia marks an extraordinary downfall for one of America's most powerful technology executives.

But behind the sensational headlines about his affair with a woman suspected of working for Chinese intelligence – a so-called honey trap – lies something potentially far more consequential: one of the most damaging American counterintelligence failures in recent memory.

And remarkably, Huang may never have knowingly betrayed a single American secret.

A successful espionage operation does not always require recruiting a willing spy. Sometimes the objective is access, sometimes influence, and sometimes stealing technology.

Sometimes the greatest victory is simply damaging an adversary's most strategically important institutions and reputation. Beijing may have achieved all four with Nvidia and the United States.

How deeply Alice Huang penetrated Jensen Huang's world

The first unanswered question is how deeply Alice Huang penetrated Jensen Huang's world.

We know the two developed an intimate relationship. What we do not know is whether she gained access to his personal telephone, computer, electronic communications, business discussions, or confidential information.

Those questions are all critical. Modern intelligence services do not necessarily need to steal documents from a locked safe.

Access to someone's smartphone, messaging applications, cloud accounts or business correspondence can potentially reveal extraordinary quantities of sensitive information.

That is why the U.S. and other NATO countries routinely warn their government personnel, and those working in defense sectors, to “leave media behind” when traveling to China. Everyone knows it; not everyone practices it.

Given the level of access this particular Chinese agent – allegedly a recruited MSS operative, Alice Huang – had to this CEO, we can only imagine the danger.

What might the chief executive of Nvidia discuss privately and unguardedly with someone he was intimate with: advanced chip development, American export restrictions, negotiations between Beijing and Washington (he learned while on Air Force One?), or corporate technology strategies and relationships with the world's leading AI companies?

> Personal relationships can provide intelligence access that even sophisticated cyberattacks struggle to achieve

And we can only imagine, and investigators need to determine, what was on his phone, laptop, or other device.

CI professionals in the FBI and at Nvidia itself must be horrified as they contemplate how much unrestricted access she had to his personal and digital media when he was sleeping, distracted, or indisposed, and for how long.

It takes only seconds, literally, for Chinese intelligence to swipe a device and download all its contents. Seconds. She had MSS gear to do it and potential access to Huang.

Even without obtaining classified government information (because presumably Jensen Huang at least – we hope – didn’t carry that in any digital or hard form), Beijing could still gain an incredible amount of intelligence from NVIDIA’s plans, intentions, and corporate secrets through her conversations with him.

As I explained in my earlier article, human

intelligence operations exploit precisely these kinds of vulnerabilities.

Personal relationships can provide intelligence access that even sophisticated cyberattacks struggle to achieve.

This could be the greatest compromise of this case. As the ole tale from the Bible cautions, the Philistines used Delilah to learn the secret of Samson's hair, which was his strength. What did Alice Huang learn to help her Chinese masters, and what might it cost U.S. national security?

Did the intelligence community adequately warn Nvidia?

The second question is whether American authorities failed to protect a critical national-security asset.

According to reporting from The New York Times and other sources, President Donald Trump was briefed on intelligence concerns about Alice Huang, yet apparently took no meaningful protective action.

We also know his administration supported expanding certain advanced Nvidia chip sales to China. Why?

Did the intelligence community adequately warn Nvidia? Were appropriate protective measures considered? Did political or commercial considerations override legitimate counterintelligence concerns?

> Better targeting, autonomous systems, and faster battlefield decisions can translate directly into American lives lost

These are not partisan questions. They concern the fundamental responsibility of any American administration to protect technologies vital to national defense.

Nvidia is not simply another technology company. Its advanced processors are foundational to the development of artificial intelligence, which increasingly underpins intelligence collection, cyber operations, weapons systems and military decision-making.

If America is potentially forced into a war with China over Taiwan – to defend its freedom or navigation in the Taiwan Strait – the consequences could be devastating.

American soldiers, sailors and airmen could face Chinese military systems enhanced by precisely the advanced AI capabilities Washington has sought to protect.

Better targeting, autonomous systems, and faster battlefield decisions can translate directly into American lives lost.

How much advanced American technology has already reached China?

And that brings us to perhaps the most disturbing question: how much advanced American technology has already reached China?

Recent reporting alleges that a network of companies associated with Alice Huang helped ship approximately 240,000 Nvidia chips, valued at some $7.5 billion, to Chinese customers. If substantiated, these revelations would be staggering.

Investigators must determine how many chips were transferred, which models were involved, whether American export restrictions were violated, and ultimately who received them.

> The MSS underwent a major reorganization in 2018, so some of these affiliations have changed, but their mission remains the same

Was Megaspeed merely a commercial enterprise exploiting profitable opportunities? Or was some portion of this business knowingly supporting Chinese intelligence objectives?

Those questions remain unresolved. But intelligence services have long exploited ostensibly legitimate commercial entities to acquire restricted technologies, obscure transactions and facilitate covert procurement.

Russian and Soviet “Line X” intelligence officers have done so for generations. China’s MSS former Bureau 12 targeted companies and influential CEOs for just this type of operation, as does Bureau 2, foreign intelligence.

The MSS underwent a major reorganization in 2018, so some of these affiliations have changed, but their mission remains the same.

What Beijing considers its greatest victory?

The final question is what Beijing considers its greatest victory. Was it access to America's most influential AI executive? The potential acquisition of sensitive information? The alleged movement of advanced processors into China? Or the destruction of Huang's leadership and the turmoil now engulfing Nvidia?

Perhaps it was a combination; or perhaps they didn’t realize even how far it could go till this past week.



The question now is not merely whether China recruited an American spy. It is whether Beijing achieved a strategic intelligence victory without ever needing one

China has denied the espionage allegations, and we still lack definitive public evidence establishing what Alice Huang provided to Chinese intelligence.

Nvidia has likewise said it has no reason to believe corporate secrets were compromised.

Those qualifications matter. But they do not diminish the seriousness of the counterintelligence questions now confronting Washington.

Still, it is a win for China; we should make no mistake there. And a giant win for Chinese intelligence.

What makes this episode extraordinary is not the alleged sexual relationship. Such techniques are centuries old.

It is the potentially catastrophic intersection of espionage, personal vulnerability, advanced technology, and national defense.

Huang has lost his position as CEO. But the consequences for American security may prove far greater.

The question now is not merely whether China recruited an American spy. It is whether Beijing achieved a strategic intelligence victory without ever needing one.

Sean Wiswesser is a former CIA Senior Operations Officer and an expert on Russian

Intelligence, Espionage, and Defense Issues.