Does China's New J-20 Stealth Fighter Have U.S. Technology?

James A. Lewis

January 26, 2011

China's military sent a signal to Secretary of Defense Robert Gates when it unveiled its new J-20 stealth fighter rolling up and down a runway just before his visit. We do not actually know how stealthy the J-20 is, but aviation experts were generally surprised that China was able to develop this advanced an aircraft as quickly as it did. Some immediately suspected that China had illicitly acquired U.S. technology to help accelerate its own programs. The Chinese, of course, deny this.

The denial counts for very little. We cannot expect a black and white case where close examination of the J-20 would reveal parts stamped "made in USA" on the aircraft. But we can compile a set of suggestive incidents that point to China's use of U.S. technology.

This is not the first time China has moved more rapidly in building advanced weaponry. It took the United States and the Soviet Union several decades to achieve reductions in the noise emitted by their nuclear submarines, while China achieved similar results in roughly a half the time. Since China does not show similar stellar performance in efforts to develop other advanced technologies—in fact, it tends to be somewhat slower—it is reasonable to ask if China was able to acquire the necessary submarine technologies, which neither the United States nor the Russians would share, through espionage or other illicit means.

We are helped in this analysis by having some knowledge of Chinese acquisitions goals for their espionage programs. This knowledge is derived from the activities of arrested Chinese spies and from their cyber-espionage targets. Stealth, advanced naval technologies (including submarine technology), sensors, and military space are high on their acquisitions list. Nuclear technologies were once at the top of the list, but the Chinese are perhaps now less interested in nuclear because they have already extracted everything of value from the United States.

China is an avid user of open source information (e.g., publicly available material) and presumably uses open source to inform and guide espionage activities collection—a published article can suggest, people, locations, and processes to target for clandestine collection. This is not an argument for publishing less; the United States has wrestled with how to control scientific research since the Reagan administration's NSDD-189, and the conclusion ever since then is that we gain more from openness than we lose.

China specifically denies that it obtained pieces of an USAF F-117 Stealth aircraft shot down by the Serbs in 1999. This denial is specious. The Serbs retained large portions of the aircraft. China was aiding Serbia in the conflict (it has a signals intelligence unit in Belgrade collecting NATO radio traffic). What better way to repay a friend than by sharing the windfall. It is also likely the Serbs offered aircraft remnants to the Russians, and they may even have been willing to sell it on the black market. This sort of sharing would not be unusual.

We know from an earlier incident when a Chinese rocket carrying a U.S. satellite exploded on launch, that the Chinese deployed hundreds of people to creep around the crash site to pick up pieces of the launcher and the satellite. This too is normal practice, an effort to determine what went wrong with the launch, but the Chinese collected pieces of the American satellite as well and subjected them to various tests in an effort to understand how they worked.

China's aircraft industry has benefited from its commercial ties to the West. When McDonnell Douglas assembled passenger aircraft in Shanghai in the early 1990s, the Chinese learned how to improve in two ways. First, when the plant was unoccupied, Chinese personnel photographed and measured all the manufacturing equipment. Second, just by working in a U.S. plant, individual Chinese learned advanced practices and skills that they could then transfer to their own companies. This learning process continues in the joint aircraft ventures Western firms have in China, and the quality of Chinese aircraft manufacturing has improved rapidly because of this technology transfer.

This is part of the Faustian bargain Western companies made to gain access to China. China's decision in the 1980s to let Western companies enter was accompanied by another decision that directed Chinese firms to acquire. Technology transfer to Chinese partners has been a part of every major business negotiation in China. Western companies have tried a series of dodges—reserving some technology to themselves, denying Chinese partners complete access, or keeping key processes outside of China. These may slow Chinese acquisitions, but they certainly do not stop them. When we see major Chinese firms using Western intellectual property without penalty to build competing products, whether it is telecom or high-speed trains, it is hard to accept that this is not a formal government program.

Western companies also say that while the Chinese may steal intellectual property, it takes them several years to turn that into a product, and by then the Western company will have introduced something newer. This is not true for all products, unfortunately, as some do not change that fast. It ignores the competitive improvements in Chinese production. For military technology, where the United States still uses equipment and devices from the 1980s and 1990s, China has been able to close the technology gap much more rapidly than expected. And this process is not helped by the general decline in our national productive capabilities.

Technology transfer to China that expanded China's productive capabilities would be in the West's interest if two conditions were met. The first is a respect for intellectual property so that Chinese firms do not copy foreign products. This was one of China's commitments in joining the World Trade Organization, which opened foreign markets to their exports, and while there has been some progress, it is not enough. The second condition is that China's larger intentions in modernizing should not be hostile. In this, there appears to be an internal division, with some in China favoring "peaceful development," while others, particularity in the military, take a more nationalist and aggressive stance. Both conditions suggest that we can no longer be as sanguine about illicit technology acquisitions by China as we have been in the past.

In the 1980s, China also benefitted from close defense industrial ties with Israel, and there were several allegations that Israel transferred advanced military technology it had received from the United States to China. An early example involved an Israeli businessman crossing into China from Hong Kong, when it was still under British control. He was detained and searched and found to be carrying military blueprints and other design material. Israel stopped these transfers after being pressed by the United States, but the poster child for this was the Chinese J-10 fighter, which originally bore a surprising resemblance to the Israeli Lavi fighter prototype, which itself was based on the U.S. F-16. The Lavi/J-10 episode probably did not play directly in the development of the J-20, but the defense industrial cooperation did accelerate Chinese programs before they were stopped and probably involved U. S. technologies.

A more telling incident involved cyber espionage. About a decade ago, Chinese hackers allegedly broke into a U.S. military research facility at China Lake, California, and were able to acquire computer files relating to stealth technology. This was during the first great wave of cyber espionage, when U.S. networks were so poorly secured that it must have seemed like a bonanza to foreign intelligence agencies. There may have been other hacks, and it is possible that information on stealth was in some of the three to four terabytes of unclassified material that Defense Department networks lost to foreign intruders in the last decade. Data extracted from China Lake, in combination with material acquired from the downed F-117, could have provided a significant boost to any stealth program.

These anecdotes and our knowledge of Chinese espionage and technology practices point to an interesting hypothesis—that China used illicitly acquired U.S. technology in its J-20 program. We do not have sufficient data to say whether this hypothesis is true or false. Very often in espionage there is ambiguity and opaqueness that can be baffling to those accustomed to more transparent processes. The correct response to this hypothesis, whether it is true or false, is not to bemoan the loss, to blame China for acting like any reasonable nation (they are not the only ones to take military technology from the United States), or to seek evidence that would "stand up in court." The correct response is to say that there are indicators we cannot safely ignore that poor cybersecurity and weak responses to economic espionage have created an opportunity for significant intelligence breaches that we would be well advised to remedy.

James A. Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, D.C.