China Builds Military Hardware With Designs And Technology Stolen From U.S.

TN Note: Technocrats in China have no moral dilemma in stealing designs and technology from other parties, especially from the U.S., where most of the state-of-the-art military hardware has been developed. Why? When technology exists for technology's sake, then it is treated as if it is in the "public domain" and hence, available for the taking. This writer has had a relationship with a tenured professor of Aeronautical Engineering at a major eastern University, who broke a ring of Chinese espionage that was blatantly stealing technology. It was known to be a wide-spread practice and the U.S. government basically turned a blind eye to the practice.

China's vibrant military blogosphere presented a video this month revealing a missile-firing unmanned aerial vehicle in action, dropping bombs against ground targets.

The Caihong-4, or CH-4, unmanned aerial vehicle (UAV) is a testament

to the remarkable success of China's military in copying vital high-technology weapons that currently are considered among the most cutting edge arms systems used in modern combat operations for both ground strikes and intelligence-gathering.

he one-minute, 37-second online posting shows takeoffs and landings of the drone. It was uploaded to the video-sharing website Youku Dec. 17. According to the blogger who posted it, the video was produced by 11th Academy of the China Aerospace Science and Technology Corporation, a drone developer and manufacturer.

The drone is shown launching two different types of bombs and the impact of their explosions on the ground. One is labeled a 50 kilogram, satellite-guided bomb and the second is an unguided CS/BBE2 50 kilogram aerial fragmentation bomb.

Photo analysis of the CH-4 shows the remote-controlled aircraft is very similar to the US military's front-line combat UAV, the MQ-9 Reaper.

Both aircraft are about the same size and wing-span and both sport identical V-tails, landing gear, imaging pods and propeller-driven rear engines.

The only major difference is the Predator's engine intake is located on top of the aircraft while the CH-4's is underneath.

There is no evidence the Chinese directly stole design information through cyber attacks against the Reaper manufacturer, General Atomics Aeronautical Systems, Inc.

But in the words of a former National Security Agency director, retired Gen. Keith Alexander, the likelihood exists Beijing acquired drone designs and technology through cyber espionage. "There are two types of companies: those that have been hacked, and know it, and those that have been hacked and don't know it," Alexander said in a recent speech.

The Pentagon's Defense Science Board warned in a 2012 report on automated defense systems that China was aggressively pursuing unmanned aircraft development and were "copying other successful

designs" to speed up their drone programs. "The scope and speed of unmanned-aircraft development in China is a wake up call that has both industrial and military implications," the report said.

China in 2012 lagged behind US drone programs but has "clearly leverage all available information on Western unmanned systems development."

In three years since the report was published the Chinese have managed to close the gap with the United States on drone development.

Additionally, Chinese military writings also indicate Beijing is working to counter US drones by interrupting their communications links. The May 2015 issue of the technical journal "Winged Missiles," published by the PLA's Electrical Engineering Institute, discussed how its done.

"Detecting a UAV system's remote link signals is important for countering UAVs," the authors note.

On Dec. 1, another Chinese website, the social media outlet Tencent News, published a report on Chinese drones, including photos of the Gongji-1 attack drone, made by the Chengdu Aircraft Industry Group. Like the CH-4, the GJ-1 bears a striking resemblance to the Reaper. The report stated that the GJ-1 has been deployed with a PLA air force UAV unit in the Gobi desert since 2012. The report showed the remotely-piloted controls and command system used by the PLA to operate the drones.

Details of pervasive Chinese military cyber theft were revealed in classified documents made public by former NSA contractor Edward Snowden.

An undated briefing slide from around 2010 titled "Chinese Exfiltrate Sensitive Military Technology" reveals that Chinese hackers had conducted more than 30,000 cyber attacks, including more than 500 described as "significant intrusions in DoD systems."

The attacks penetrated at least 1,600 network computers and compromised at least 600,000 user accounts. The damage was assessed

as costing more than $100 million to gauge the damage and rebuild the networks.

The systems compromised included a range of commands and agencies, including the US Pacific Command, the US Transportation Command, the US Air Force, US Navy including missile navigation and tracking systems and nuclear submarine and anti-air missile designs.

In all the Chinese obtained an estimated 50 terabytes of data, an equivalent to five times the holdings of the US Library of Congress, the American national library considered the second largest library in the world with 23.9 million catalogued books.

Separate NSA briefing slides identified 13 separate Chinese cyber intelligence-gathering operations that NSA traced to the 3rd Department of PLA General Staff Department, the electronic military spying service known as 3PL.

Read full story here…