

افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نیاشد تن من مباد بدین بوم ویر زنده یک تن مباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com

afgazad@gmail.com

European Languages

زبان های اروپایی

http://english.pravda.ru/world/americas/23-05-2014/127641-american_defense_contractors-0/?mode=print

American defense contractors: Profiting from Russian and Chinese technology

by John Stanton

5/23/2014

"Boeing is a leader in creating the U.S.-China Aviation Cooperation program, an initiative of U.S. government and American aviation companies, working with CAAC and airlines to help advance China's commercial aviation. Good corporate citizenship has always been an essential part of The Boeing Company. In China, the company's vision for corporate social responsibility program is to stretch Boeing expertise and commitment to the science, technology, engineering and mathematics (STEM) education of Chinese youth from elementary school to college."
Boeing in China, Backgrounder, April 14, 2014

It is a fine thing that Boeing is supporting STEM education in China. But as part of the American Defense Industrial Base Critical Infrastructure, Boeing regularly moans about the dearth of America's own STEM/ aerospace engineering capability. For example, in a glossy publication from 2007 comes the article Engineering Brain Drain? by Louise Wilkerson, in which the reader learns that "According to a recent study by Aviation Week & Space Technology magazine, the

United States is turning out only about 110,000 engineers a year compared with China's 600,000 a year and India's 350,000 a year."

Even though there is no conclusive evidence to claim there is a shortage of aerospace engineers in the USA (immigrants or not), the Pentagon and its defense contractors continue to moan and groan about a mythic shortage that does not actually exist. Perhaps Boeing is hedging its bets by financially supporting STEM in China and advanced materials and computing research there.

"Boeing has also established Boeing Research & Technology-China, a part of Boeing's advanced central research and development organization. The center is involved in collaborative research with the Chinese Academy of Sciences and Chinese universities. Three joint research laboratories and a joint research center have been formed with the research partners. Activities are focused on the environment, advanced materials, and advanced computing technologies for aviation and industry design."

One of the most sophisticated missile defense early warning platforms was constructed by Boeing. The company's Sea Based X Band radar system currently floating in the Pacific was built by Russia's Vyborg Shipyard.

According to navaltechnology.com "The Sea-Based X-Band Radar-1 (SBX-1) constitutes a mid-course fire control radar based on a seagoing semi-submersible vessel. The platform was developed by Boeing, as part of the ground-based midcourse defence (GMD) component of the US Ballistic Missile Defence System (BMDS). The GMD intercepts incoming warheads. The SBX vessel was transferred to the Military Sealift Command (MSC) in December 2011." The X Band Radar System on board was built by another Defense Industrial Base heavyweight Raytheon Corporation.

Yak, Yak

Lockheed Martin, the world's largest defense contractor, is in the news as being a victim of Chinese PLA military personnel who apparently surreptitiously entered Lockheed computer networks and engaged in industrial espionage. Yet Lockheed has been doing business with China in the area of nuclear reactor safety and construction. The F-35B has its genesis in Russia.

According to a corporate press release on Lockheed Martin's website, "Lockheed Martin and [China's] State Nuclear Power Automation System Engineering Company (SNPAS) have signed an agreement to prototype, manufacture and qualify nuclear power plant reactor protection systems for China's Generation III reactors. SNPAS is a subsidiary of China's State Nuclear Power Technology Corporation (SNPTC). Lockheed Martin and SNPAS will develop a nuclear

safety instrumentation and control platform, based on field programmable gate array (FPGA) technology, for a new generation of Reactor Protection Systems in China. Terms of the agreement were not disclosed."

It turns out that the vaunted F-35 has its origins in Russian aviation. According Aviation Intel "People look at the F-35B and see an ultra- modern transformer of sorts, with massive doors that open up and an articulated exhaust tube that seems to warp downward unnaturally on command. The next thing you know the 5th generation stealth fighter is HOVERING IN MID AIR. Lay on decent range (for a V/STOL fighter), higher than Mach speeds, and the most cutting edge radar and avionics package ever and you have a truly groundbreaking design.....But is the F-35B's unique design really that ground breaking at all? The F-35B's novel lift fan and vectoring tailpipe design was conceived not in Fort Worth, Texas but in Moscow, Russia, about 35+ years ago! The Yak-41 that utilized this exact same concept, now known as the Yak-141, NATO codename "Freestyle," was designed to be what it's much lacking Yak-38 predecessor should have been."

And maybe it is coincidence but Lockheed stands to gain big-dollar cyber security contracts from the US government.

There is something shady about spending billions on cyber offense and defense when no one seems to have a formula or can quantify how much proprietary/national security data has really been covertly compromised by the Chinese, Russians or a middle-school student located in Houston, Texas. The US government-Lockheed officials are not to be trusted. They offer dubious information that lacks specifics or legitimately quantifiable formula/data with which to assign dollar losses. It's a sham not unlike the trumped up aerospace engineering gap.

Cyber Threats are Real?

According to Tereza Pultarova, writing in Engineering and Technology Magazine (May 2014) "Speaking at the Reuters Cyber-security Summit in Washington, the company's vice president Chandra McMahan said that only since January 2014, the firm had to ward off attacks by 43 distinct hacking groups. The number of cyber-attacks on Lockheed's systems has been growing steadily - in 2007, ten attacks were detected while three years later it was already 28. In addition to being Pentagon's number one weapons supplier, Lockheed Martin is also the most important provider of information technology to the US government. The company's systems are widely used by the US military, energy companies, utilities and other critical infrastructure firms.

The latter have seen, according to Lockheed Martin, a substantial increase in the number of cyber-attacks in the past years. *"While we haven't seen specific action on objectives in terms of*

damage, what we have seen over the last several years (is) malware created and deployed to damage critical infrastructure," McMahon said... Lockheed expects double-digit growth in its cyber business, which now accounts for 10 per cent of revenues in the \$8bn (£4.77bn) information systems sector. Lockheed and other US weapons makers are frequent targets of criminal groups, nation states and other hackers seeking to extract valuable information about high-end weapons systems. US intelligence reports have cited attacks launched by groups in Iran, China, Russia and North Korea. Lockheed declined comment on any specifics about the campaigns it had identified."