Policy Brief No. 6

September 2010

China's Defense Electronics Industry: Innovation, Adaptation, and Espionage

James Mulvenon and Matthew Luce

Summary

Contrary to popular perceptions of China as either "technology thief" or "technology superpower," the success of the Chinese defense electronics sector can be attributed to a combination of indigenous innovation, adaptation of foreign technology, and large-scale technology espionage. Advanced defense electronics components and systems play a key role in this revolution in military capability, making it imperative to understand the strengths and weaknesses of the Chinese defense electronics industry and their implications for U.S. interests in the region.

The Study of Innovation and Technology in China (SITC) is a project of the University of California Institute on Global Conflict and Cooperation. SITC Policy Briefs provide analysis and recommendations based on the work of project participants. Author's views are their own.

INNOVATION, ADAPTATION, ESPIONAGE

Since the late 1990s, the Chinese military has deployed a highly advanced Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture, providing redundant, secure communications and longer-range space, air, and ground-based sensors.

For those parts of the global military revolution that rely on commercial-off-the-shelf technology (COTS), such as switches or routers, China has been able to take advantage of the globalized production and R&D chain currently based on the mainland, partner with foreign providers, modernize their production base, and begin the process of adaptation and then indigenous innovation.

For those parts of the global military revolution that have no natural analog in the commercial electronics sector, like components with radiation hardening or wide military standard temperature ranges, China has been forced to steal from abroad for either reverse engineering or inclusion in production designs. This dual-use dynamic creates significant complications for efforts at export controls and counter-proliferation, especially coordination with allies in the Wassanaar Group.

IMPLICATIONS FOR CHINESE MILITARY MODERNIZATION

Throughout its history, the People's Liberation Army (PLA) has suffered from inadequate and outdated information technology, characterized by limited capacity and lack of security. In the past, these weaknesses have severely limited the military's ability to transmit and process large amounts of information or coordinate activities among the various military regions, thereby reducing military effectiveness. For example, observers believe that inadequate communications were a major factor in the heavy losses suffered by the PLA during China's border conflict with Vietnam in 1979. In stark contrast, the PLA is very much aware of the critical role played by information-based C4ISR technologies in the 1991 Gulf War, and the importance of these technologies in securing the eventual Allied victory against a force using largely Soviet and Chinese equipment.

To overcome these deficits, the PLA has embarked on a well-financed effort to modernize its C4ISR infrastructure. Thanks to the introduction of an advanced, secure telecommunications infrastructure, the PLA has reportedly achieved significant improvement in its communications and operational security, as well as in its capacity to transmit information.

Specifically, the use of advanced optical fiber communications facilities, satellites, long-distance automated switches and computer-controlled telephone systems has significantly accelerated the Chinese armed forces' digitization process and the rapid transmission and processing of military information. The speedy development of strategic communications networks has shortened the distance between command headquarters and grassroots units, and between inland areas and border and coastal areas. Currently the armed forces' networks for data exchange have already linked up units garrisoned in all medium-sized and large cities in the country as well as in border and coastal areas.

As a result of the automated exchange and transmission of data, graphics, and pictures within the armed forces, military information can now be shared by all military units. On the sensor front, China has also made significant advances, as evidenced by the deployment of new constellations of Beidou navigation satellites, Dongfanghong/DFH-4, (Fenghuo) communications satellites, and phased-array radars.

Yet the real question is this: Will this increasingly advanced information technology system in the military merely improve the handling of information, or will it also bootstrap the PLA's much more primitive, much less "informationized" conventional forces? For the time being, the benefits seem restricted to the communications and information security arenas, and problems remain in practical operation in battle, which is the practical application of these technologies to actual warfighting capabilities. Yet the recent debate in Chinese military writings about "informationization" (*xinxihua*) provides some clues about their strategy, which appears to involve upgrading existing

mechanized systems with information technology systems rather than waiting to deploy next-generation high-tech platforms.

This is not the Revolution in Military Affairs or "network-centric warfare" as defined in the West, but a realistic use of China's growing IT capabilities to achieve short-term military capability gains. In an environment in which the United States and China continue to face the real possibility of military conflict over the Taiwan Strait, the accumulated contributions of the digital triangle could have a direct impact on U.S. military operations, national security, and the defense of allies in the region.

IMPLICATIONS FOR U.S. EXPORT CONTROL POLICIES

To blunt or counter these trends, it is tempting to consider placing export controls on information technologies to China. The inherently dual-use nature of most information technology makes nonproliferation efforts difficult, if not impossible. Moreover, the global nature of the IT industry renders most unilateral controls by the United States irrelevant. For example, even if the U.S. government can find a way to prevent Cisco from selling a system to a Chinese unit, a representative from Alcatel or Siemens will pick up the contract.

There are, of course, exceptions to this generalization. In some cases, the U.S. government may indeed have some leverage over international transfers of these technologies, and all appropriate measures should be taken. One suboptimal case is U.S. total dominance of a market, where export-control concerns need to be balanced against the possibility of giving aid and comfort to potential international competitors. A better case is the former sanctions regime in Iraq, where the UN mechanism provided a forum for preventing suspicious transfers.

RECOMMENDATIONS

1. Rather than focusing on stemming the tide of technology, it would be more productive to recognize the global proliferation of these technologies, then seek ways to exploit the proliferation to further U.S. interests. Doing so requires a three-step policy:
   b. Carry out effective tracking of these technologies, which includes a range of activities from sophisticated information collection to simply reaching out to corporate representatives in a systematic way. Indeed, most of this information can be found easily in open sources.
   c. The key to the power of these technologies is their integration, which requires a greater understanding by analysts of the technologies themselves, their limitations, and their possibilities.
   d. Rather than fight the inexorable tide of these technologies to China, use this tracking information and technical knowledge to work with industry to make sure the "right" technologies are imported to maximize U.S. options.

James MULVENON is vice president of Defense Group Inc.'s Intelligence Division, as well as co-founder and director of its Center for Intelligence Research and Analysis. His current research focuses on Chinese cyber issues, C4ISR, defense research/development/acquisition organizations and policy, strategic weapons doctrines, patriotic hackers, military leadership and corruption, and the military and civilian implications of the information revolution in China.

Matthew LUCE is a researcher and Chinese linguist at Defense Group Inc.'s Center for Intelligence Research and Analysis, where he does primary source research and analysis of China's science and technology policies and development programs. Luce's research and writing focuses on cyber security, C4ISR-related technologies, and China's ethnic relations.