US DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2011

M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems, School of Business & Management
Norwich University, Northfield VT

Contents

Introduction

The *Annual Report to Congress on the Military Power of the People's Republic of China* from the US Department of Defense has been issued every year since 2002:

> The FY2000 National Defense Authorization Act (Section 1202) directs the Secretary of Defense to submit a report "…on the current and future military strategy of the People's Republic of China [PRC]. The report shall address the current and probable future course of military-technological development on the People's Liberation Army [PLA] and the tenets and probable development of Chinese grand strategy, security strategy, and military strategy, and of the military organizations and operational concepts, through the next 20 years."
>
> This report, submitted in response to the FY2000 National Defense Authorization Act, addresses (1) China's grand strategy, security strategy, and military strategy; (2) developments in China's military doctrine and force structure, to include developments in advanced technologies which would enhance China's military capabilities; and, (3) the security situation in the Taiwan Strait.[1]

Reading through all the reports from 2002 through 2011 provides valuable perspective on the DoD view of Chinese information warfare capabilities. The following is a simple compilation of extracts from the *Annual Reports* bearing on information warfare capabilities and commitment of the PRC and the PLA, including specific commentary about industrial espionage sponsored by agencies in the PRC.

[1] (US Department of Defense 2009)

2002

- "Information Warfare. To improve its skill base, the PLA [People's Liberation Army] has been recruiting specialists via its reserve officer selection program in order to design, comprehend, and execute a full-spectrum information operations/information warfare (IO/IW) campaign."[2]

2003

- "The PRC's efforts to develop, acquire and gain access to advanced technologies that would enhance military capabilities are multi-faceted and include the use of traditional military actors, commercial entities, and individuals involved in basic scientific research. The production of advanced weapon systems requires not only the transfer or development of the technology, but also the transfer or development of associated knowledge, including training, education, technical skills, and manufacturing know-how."
- "In 1979, China began modernizing its weapons facilities through a policy emphasizing production of both military and civilian goods throughout its defense industrial base. This policy shift reflects China's aspiration to attain long-term self-sufficiency through the acquisition of key foreign dual-use technologies and knowledge. Once such technology is obtained, defense-affiliated institutes and factories may apply them to the design and production of commercial and/or military end-items. Moreover, design and production of commercial goods by the defense industrial base can generate revenue and foreign exchange to finance the acquisition of advanced technology. Since 1979, thousands of PRC business entities have been established in the United States. The bulk of the business conducted by these entities is probably legitimate, but an undetermined number may target dual-use commodities and controlled technologies restricted from sale to the PRC. Authoritative PRC journals have recommended an increase in the use of overseas ethnic-Chinese scientists to transfer foreign technology."
- "Using academic exchange as a medium to train scientists and to develop ties between scientists, China appears to be building an informal science and technology (S&T) network around the world that could not only contribute to basic research but also to the development of commercial and military technologies. One example of a military significant S&T collection involves two Chinese students at two prominent U.S. universities collecting information regarding Terfenol-D. Terfenol-D is a rare earth metal developed by the Department of Energy's Ames Laboratories which is used in militarily critical naval and aerospace applications. Although one of the Chinese students admitted sending this information to the PLA, usually the connections between academic, commercial, and military organizations are not so clear cut. The close relationships between the personnel and organizations involved often makes it difficult to separate the research, funding, and cooperation triangle among Chinese universities, government institutes, and businesses."[3]

2004

- "China is experiencing a rapid buildup of its information technology capabilities. The Chinese government effectively uses market access and regulations to force major foreign information technology companies to transfer technology, share know- how, and, more recently, open research and development labs in China. Many of the Chinese companies in

[2] (US Department of Defense 2002)
[3] (US Department of Defense 2003)

these joint ventures are affiliated with state research institutes under the Ministry of Information Industry or the PLA's General Staff Department. As a result of these trends, China is acquiring the personnel and technology bases for a credible computer network operations capability."

- "Electronic warfare (EW) is an important aspect of the PLA's combat operations and is viewed as crucial to achieving information dominance in the battlespace. The PLA is believed to be able to conduct both defensive and offensive EW operations. Basic objectives of an electronic attack campaign are to conceal PLA operational preparations, weaken enemy air defense early warning, and paralyze or disrupt enemy integrated air defense systems. Chinese electronic warfare operational concepts emphasize concealing the activities and disposition of PLA forces and misleading the enemy. Electronic attack can deceive or desensitize enemy battle commanders through insertion of spurious radar tracks or blot out entire avenues of approach. China's EW modernization program consists of foreign technology procurement, reverse engineering, and parallel domestic research and development programs. The Chinese intend to accelerate modernization through technological leapfrogging. Beijing may bypass phases of equipment development by purchasing commercial-off-the-shelf technology."[4]

2005

- "China's computer network operations (CNO) include computer network attack, computer network defense, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and "electromagnetic dominance" early in a conflict, and as a force multiplier. Although there is no evidence of a formal Chinese CNO doctrine, Chinese theorists have coined the term "Integrated Network Electronic Warfare" to describe the Chinese approach. This concept outlines the integrated use of electronic warfare, CNO, and limited kinetic strikes against key C4 nodes to disrupt the enemy's battlefield network information systems. The PLA has likely established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics to protect friendly computer systems and networks. The PLA has increased the role of CNO in its military exercises. Although initial training efforts focused on increasing the PLA's proficiency in defensive measures, recent exercises have incorporated offensive operations, primarily as first strikes against enemy networks."[5]

[4] (US Department of Defense 2004)
[5] (US Department of Defense 2005)

2006

- "As its domestic defense industry matures, China is actively seeking foreign weapons and technology, primarily from Russia and states of the former Soviet Union, to fill near-term capability gaps. In the long term, however, Beijing seeks to establish a wholly indigenous defense industrial sector. China's military industrial base also benefits from foreign direct investment and joint ventures in the civilian sector, the technical knowledge and expertise of students returned from abroad, and industrial espionage."
- "Most of China's defense industries rely on foreign procurement and development. The exceptions are few, e.g., ballistic missiles and some space and aviation programs. Civilian industrial reform has advanced more quickly than the military sector because it can attract foreign investment with fewer restrictions. However, foreign investment in physical plant, management, technical, and marketing expertise in some basic manufacturing sectors, such as strategic metals and electronics, has increased the prospect for spin-off with military and dual-use industries.
- Joint ventures in China also now manufacture semiconductors and integrated circuits used in military computers, communications and electronic warfare equipment, and missile guidance and radar systems.
- Many of China's new generation of scientists, engineers, and managers receive training and have experience in the United States and other countries. In 2004, the United States granted 35,578 F-1, J-1, and M-1 student or exchange visas to PRC nationals, according to the Department of Homeland Security, Office of Immigration Statistics.
- China also continues to acquire key technologies and manufacturing methods independent of formal contracts. Industrial espionage in foreign research and production facilities and illegal transfers of technology are used to gain desired capabilities. Where technology targets remain difficult to acquire, foreign investors are attracted to China via contracts that are often written to ensure Chinese oversight, with the eventual goal of displacing foreigners from the companies brought into China."[6]

[6] (US Department of Defense 2006)

2007

- "In 2005, China signed arms agreements with foreign suppliers worth almost $2.8 billion, making it the third largest arms recipient among developing countries. Russia remains China's primary weapons and materiel provider, selling it advanced fighter aircraft, missile systems, submarines, and destroyers. China is currently negotiating the purchase of additional surface-to-air missiles, combat aircraft, aircraft engines, and assault and transport helicopters. China relies on Russian components for several of its production programs and has purchased production rights to Russian weapon designs. Russia cooperates with China on technical, design, and material support for numerous weapons and space systems; for example China's *Shenzhou* manned space module is based on the Russian *Soyuz* capsule.
- Israel has also historically been a supplier of advanced military technology to China. The Israelis transferred HARPY UCAVs to China in 2001 and conducted maintenance on HARPY parts during 2003-2004. In 2005, Israel began to improve government oversight of exports to China by strengthening controls of military exports, establishing controls on dual-use exports, and increasing the role of the Ministry of Foreign Affairs in export-related decisions. In January 2007, Israel implemented new dual-use export controls, based on the Wassenaar Arrangement. As of February 2007, legislation pending in the Knesset would adopt Wassenaar controls on munitions list exports. It remains unclear to what extent the new export controls will prevent additional sensitive military-related transfers to Beijing in the future.
- Despite their history of strong arms trade relationships with China, Russia and Israel have usually refrained from transferring their most sophisticated weapons systems to China. To diversify its arms supplier base and acquire advanced technology, the PRC is looking to alternative suppliers such as Europe. Since 2003 China has been pressuring EU states to lift the embargo on lethal military sales to China that the EU imposed in response to the PRC's 1989 crackdown on Tiananmen Square demonstrators. In their Joint Statement following the 2004 EU-China Summit, European leaders committed to work towards lifting the embargo, a pledge they repeated in 2005 and 2006."
- "China continues a systematic effort to obtain from abroad through legal and illegal commercial transactions dual-use and military technologies. Many dual-use technologies, such as software, integrated circuits, computers, electronics, semiconductors, telecommunications, and information security systems, are vital for the PLA's transformation into an information-based, networkcentric force. Several high profile legal cases highlight China's efforts to obtain sensitive U.S. technologies (e.g., missile, imaging, semiconductor, and submarine) illegally by targeting well-placed scientists and businessmen. U.S. Immigration and Customs Enforcement (ICE) officials have rated China's aggressive and wide-ranging espionage as the leading threat to U.S. technology. Since 2000, ICE has initiated more than 400 investigations involving the illicit export of U.S. arms and technologies to China."[7]

[7] (US Department of Defense 2007)

2008

- "Officials from the Federal Bureau of Investigations (FBI) have identified China as running an aggressive and wide-ranging effort aimed at acquiring advanced technologies from the United States. Similarly, officials from U.S. Immigration and Customs Enforcement (ICE) have referred to China as the leading espionage threat to the United States. Between 2000 and May 2006, ICE initiated more than 400 investigations involving the illicit export of U.S. arms and technologies to China.
- In December 2007, a California resident was sentenced to two years in prison and fined for his role in a scheme to export night vision technology illegally to the PRC.
- The former director of a research institute associated with Russia's space agency was sentenced to eleven and one-half years in prison for passing classified technology to China. According to a Russian spokesperson, the information could be used to create missiles capable of carrying nuclear warheads."
- "As China's defense industries develop, the PLA is relying on acquisition of foreign weapons and technology, primarily from Russia, to fill near-term capability gaps. China also harvests spin-offs from foreign direct investment and joint ventures in the civilian sector, technical knowledge and expertise of students returned from abroad, and state-sponsored industrial espionage to increase the level of technologies available to support military research, development, and acquisition. Beijing's long-term goal is to create a wholly indigenous defense industrial sector able to meet the needs of PLA modernization as well as to compete as a top-tier producer in the global arms trade. China is already competitive in some areas, such as communications, with leading international defense firms."
- "China continues a systematic effort to obtain dual use and military technologies from abroad through legal and illegal commercial transactions. Many dual-use technologies, such as software, integrated circuits, computers, electronics, semiconductors, telecommunications, and information security systems, are vital for the PLA's transformation into an information-based, network-enabled force. Several high-profile legal cases highlight China's efforts to obtain sensitive U.S. technologies (e.g., missile, imaging, semiconductor, and submarine) illegally by targeting well-placed scientists and businessmen. ICE officials have rated China's aggressive and wide-ranging espionage as the leading threat to U.S. technology. Between 2000 and May 2006, ICE initiated more than 400 investigations involving the illicit export of U.S. arms and technologies to China, which led to several convictions of U.S.-based violators of the Export Administration Act and the Arms Export Control Act.
- Key areas where China continues to rely most heavily on foreign technologies include guidance and control systems, turbine engine technology, and enabling technologies such as precision machine tools and advanced diagnostic and forensic equipment, applications and processes essential to rapid prototyping, computer-assisted design/manufacturing (CAD/CAM) and reverse engineering."[8]

[8] (US Department of Defense 2008)

2009

- "PRC military writings highlight the seizure of electromagnetic dominance in the early phases of a campaign as among the foremost tasks to ensure battlefield success. PLA theorists have coined the term "integrated network electronic warfare" (*wangdian yitizhan* - 网电一体战) to describe the use of electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield network information systems that support an adversary's warfighting and power projection capabilities. PLA writings on future models of joint operations identify "integrated network electronic warfare" as one of the basic forms of "integrated joint operations," suggesting the centrality of seizing and dominating the electromagnetic spectrum in PLA campaign theory."
- "In 2003, the CCP Central Committee and the CMC approved the concept of "Three Warfares" (*san zhong zhanfa* - 三种战法), a PLA information warfare concept aimed at influencing the psychological dimensions of military activity:
    - **Psychological Warfare** seeks to undermine an enemy's ability to conduct combat operations through psychological operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations.
    - **Media Warfare** is aimed at influencing domestic and international public opinion to build public and international support for China's military actions and to dissuade an adversary from pursuing policies perceived to be adverse to China's interests.
    - **Legal Warfare** uses international and domestic laws to gain international support and manage possible political repercussions of China's military actions."
- "The PLA is investing in electronic countermeasures, defenses against electronic attack (e.g., electronic and infrared decoys, angle reflectors, and false target generators), and Computer Network Operations (CNO). China's CNO concepts include computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. In 2005, the PLA began to incorporate offensive CNO into its exercises, primarily in first strikes against enemy networks."
- "According to a 2008 Federal Bureau of Investigation (FBI) statement, PRC intelligence services "pose a significant threat both to the national security and to the compromise of U.S. critical national assets," and concluded that these services "will remain a significant threat for a long time." The U.S. intelligence community has noted that, of all foreign intelligence organizations attempting to penetrate U.S. agencies, China's are the most aggressive."
- "China has also identified 16 "major special items" for which it plans to develop or expand indigenous capabilities. These include core electronic components, high-end universal chips and operating system software, very large-scale integrated circuit manufacturing, next-generation broadband wireless mobile communications, high-grade numerically controlled machine tools, large aircraft, high-resolution satellites, manned spaceflight, and lunar exploration."
- "Shu Quansheng, a naturalized U.S. citizen • who worked as a physicist in the United States, pleaded guilty to violating the Arms Export Control Act by providing the PRC with information on the design and development of a fueling system for space launch vehicles.

- Chi Mak, a PRC national, acknowledged being • placed in the United States for more than 20 years to conduct espionage against the United States, providing sensitive plans for U.S. Navy ships, submarines, and weapons to the PRC. In March 2008, he was sentenced to twenty-four and a half years in prison by a federal judge.
- In April 2008, Indian Government officials confirmed that its Ministry of External Affairs' computer network and servers were the victims of intrusions that appeared to originate in China.
- In May 2008, the Belgian Government reported that it had been targeted by PRC hackers multiple times.
- In May 2008, U.S. authorities investigated whether PRC officials secretly copied contents of a U.S. Government laptop during a visit to China by the U.S. Commerce Secretary and used the information to try to penetrate into Commerce computers. The investigation is ongoing."[9]

2010

- In 2009, numerous computer systems around the world, including those owned by the U.S. Government, continued to be the target of intrusions that appear to have originated within the PRC.
- These intrusions focused on exfiltrating information, some of which could be of strategic or military utility. The accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. It remains unclear if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the PRC government. However, developing capabilities for cyberwarfare is consistent with authoritative PLA military writings.
- In March 2009, Canadian researchers uncovered an electronic spy network, apparently based mainly in China, which had reportedly infiltrated Indian and other nations' government offices around the world. More than 1,300 computers in 103 countries were identified."[10]

[9] (US Department of Defense 2009)
[10] (US Department of Defense 2010)

2011

- "Cyberwarfare Capabilities. In 2010, numerous computer systems around the world, including those owned by the U.S. Government, were the target of intrusions, some of which appear to have originated within the PRC. These intrusions were focused on exfiltrating information. Although this alone is a serious concern, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. China's 2010 Defense White Paper notes China's own concern over foreign cyberwarfare efforts and highlighted the importance of cyber-security in China's national defense.
- Cyberwarfare capabilities could serve PRC military operations in three key areas. First and foremost, they allow data collection through exfiltration. Second, they can be employed to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict.
- Developing capabilities for cyberwarfare is consistent with authoritative PLA military writings. Two military doctrinal writings, Science of Strategy, and Science of Campaigns identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe. Although neither document identifies the specific criteria for employing computer network attack against an adversary, both advocate developing capabilities to compete in this medium.
- The Science of Strategy and Science of Campaigns detail the effectiveness of IW and computer network operations in conflicts and advocate targeting adversary command and control and logistics networks to impact their ability to operate during the early stages of conflict. As the Science of Strategy explains, —In the information war, the command and control system is the heart of information collection, control, and application on the battlefield. It is also the nerve center of the entire battlefield.‖
- In parallel with its military preparations, China has increased diplomatic engagement and advocacy in multilateral and international forums where cyber issues are discussed and debated. Beijing's agenda is frequently in line with the Russian Federation's efforts to promote more international control over cyber activities. China has not yet agreed with the U.S. position that existing mechanisms, such as International Humanitarian Law and the Law of Armed Conflict, apply in cyberspace. China's thinking in this area is evolving as it becomes more engaged."[11]

[11] (US Department of Defense 2011)

Works Cited

US Department of Defense. "Annual Report on the Military and Security Developments Involving the People's Republic of China 2010." *US Department of Defense.* 2010. http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military and Security Developments Involving the People's Republic of China 2011." *US Department of Defense.* 2011. http://www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2002." *US Department of Defense.* 2002. http://www.defense.gov/news/Jul2002/d20020712china.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2003." *US Department of Defense.* 2003. http://www.defense.gov/pubs/2003chinaex.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2004." *US Department of Defense.* 2004. http://www.defense.gov/pubs/d20040528PRC.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2005." *US Department of Defense.* 2005. http://www.defense.gov/news/Jul2005/d20050719china.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2006." *US Department of Defense.* 2006. http://www.defense.gov/pubs/pdfs/China%20Report%202006.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2007." *US Department of Defense.* 2007. http://www.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2008." *US Department of Defense.* 2008. http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf (accessed 12 30, 2012).

—. "Annual Report on the Military Power of the People's Republic of China 2009." *US Department of Defense.* 2009. http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf (accessed 12 30, 2012).

—. "Annual Report to Congress: Military Power of the People's Republic of China." *US Department of Defense.* 2009. http://www.defense.gov/pubs/china.html (accessed 12 30, 2012).

