

### SECTION 3: THE NATURE AND EXTENT OF CHINA'S SPACE AND CYBER ACTIVITIES AND THEIR IMPLICATIONS FOR U.S. SECURITY

“The Commission shall investigate and report exclusively on—

...

“REGIONAL ECONOMIC AND SECURITY IMPACTS—The triangular economic and security relationship among the United States, [Taiwan], and the People's Republic of China (including the military modernization and force deployments of the People's Republic of China aimed at [Taiwan]), the national budget of the People's Republic of China, and the fiscal strength of the People's Republic of China in relation to internal instability in the People's Republic of China and the likelihood of the externalization of problems arising from such internal instability. ...”

#### Introduction

China's government is devoting a great deal of attention and resources to developing outer space and cyber space capabilities. China's military strategists view the U.S.' dependence on space assets and information technology as its “soft ribs and strategic weaknesses.”<sup>157</sup> These investments by China's military potentially could provide it with an asymmetric\* capability enabling it to prevail in a conflict with U.S. forces.

China's developments in these fields are significant and have affected other nations. For example, German Prime Minister Angela Merkel complained during a trip to China in 2007 about cyber intrusions of German government computers she said originated in China.<sup>158</sup>

#### China's Space Program

China's space program consists of a wide range of activities, including military intelligence and reconnaissance, earth monitoring, research and development, scientific exploration, communications and media, and military command and control. The program contributes to the country's military power, economic development, and internal stability.<sup>159</sup> One facet of the space program is pro-

\*Asymmetric is defined as “systems to leverage China's advantages while exploiting the perceived vulnerabilities of potential opponents.” Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China, 2005*.

viding increased capabilities to the People's Liberation Army (PLA) to collect and exploit battlefield information.<sup>160</sup> Other facets, such as China's kinetic antisatellite (ASAT) system and a variety of non-kinetic space weapons, increase the offensive ability of China's forces and consequently their ability to dominate the battle space.<sup>161</sup>

China's space program earns revenue by providing launch services for other countries such as Brazil, Venezuela, and Nigeria. The investments China makes in its space program stimulate innovation, which in turn creates new technologies<sup>162</sup> that can satisfy both domestic needs and the product needs of China's exporting industries. Economic growth is viewed by the Chinese leadership as inextricably linked to its legitimacy and political monopoly. Additionally, the space program indirectly promotes internal stability by enhancing the prestige of the Chinese government and increasing national pride. Applications of the space program increase the government's ability to respond to domestic unrest or natural disasters.<sup>163</sup> For example, through earth monitoring the government can map and track the impact of floods, typhoons, earthquakes, and other disasters and any resultant population movements.

In broad terms, China's space program benefits China internationally as well as domestically. It does so by improving the nation's technology base and thereby enabling China to engage in and influence global commerce, communications, and technology development. This allows China to work toward its larger strategic goal of becoming an international power<sup>164</sup> and, as described by Ashley Tellis of the Carnegie Endowment for International Peace, it helps China in "recovering the greatness that China enjoyed internationally for most of the last millennium."<sup>165</sup>

Although there has been a wide consensus internationally with respect to the definition and limitations of sovereignty and appropriate activity in space since the adoption of the 1967 Outer Space Treaty, China—the world's newest space-faring nation—has begun to assert new views of sovereignty in outer space. Jim Lewis of the Center for Strategic and International Studies and Phillip Meek of the U.S. Air Force addressed these issues for the Commission. They explained how China uses "legal warfare" or "lawfare" as a preemptive strategy for advancing its positions on outer space. For example, one Chinese author argues that "there is no clear standard in international law as to the altitude to which territorial space extends."<sup>166</sup> (For a more detailed discussion of this issue, see chap. 2, sec. 2, "China's Views of Sovereignty and Methods of Controlling Access to its Territory.")

### ***The Characteristics of China's Space Program***

China became the world's third space-faring nation in October 2003, when it put a man into space using its own rocket. Two years later, in October 2005, it sent two "taikonauts" into space on the Shenzhou VI spacecraft. China's third manned mission occurred in September 2008 and included the first extravehicular activity (i.e., "spacewalk") by Chinese taikonauts.<sup>167</sup> China already has a space vehicle orbiting the moon and plans to explore the lunar surface with a remote rover vehicle around 2015, with possible manned missions after that.<sup>168</sup>

Today, China's space program is comprehensive and incorporates all features from design to launch, and from managing exploitation of space assets to controlling their operation.<sup>169</sup> The country's large and well-diversified research and development base currently has approximately 200,000 engineers working in various disciplines, to include space nuclear power, propulsion, materials, multispectral sensors, and robotics.<sup>170</sup> In addition,

- China launched its first data relay and tracking satellite in April 2008, giving its military real-time intelligence and collection capability.

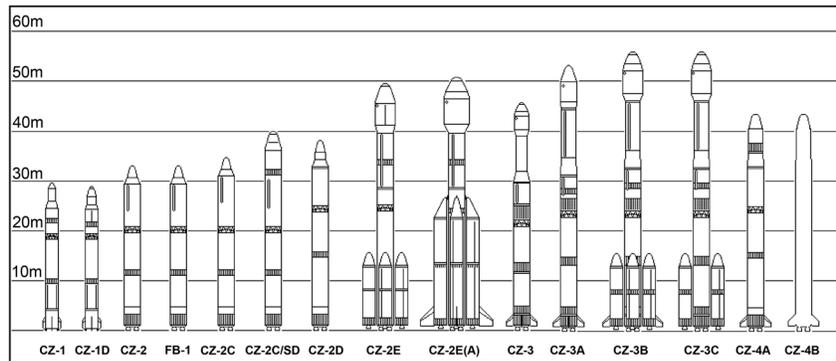
#### **MILITARY USES OF SATELLITES** <sup>171</sup>

- **imagery:** purposes range from identifying targets to detecting the effects of underground nuclear detonations.
- **navigation:** purposes range from locating targets to guiding weapon systems. There are two main global navigation systems: the U.S. military's global positioning system, or GPS, and the Russian GLONASS system.
- **signals intelligence (SIGINT):** purposes range from detecting to capturing communications, including broadcasting signals.
- **telecommunications (telecoms):** in military operations, purposes include enabling exchange of information between "front-line" and strategic commanders.
- **early warning:** the purpose is to use infrared sensors to spot missile launches by detecting their infrared signatures.
- **meteorology:** the purpose is to collect weather data, enabling meteorologists to provide more accurate forecasts for the military.

Satellites relay data to ground stations where the data are processed.

- China's military space program possesses a number of space launch vehicles with varying capabilities. There are many different configurations of its Long March Series capable of supporting different payloads. Space launches currently are supported by three different launch facilities. China's Pioneer rocket has demonstrated a mobile launch capability.<sup>172</sup>

Family of Chinese Long March Rockets



Source: Federation of American Scientists, April 20, 2005.

- The PLA utilizes an extensive network of ground-based stations for space tracking and data processing. These facilities are spread throughout the country. Supplementing these are four ships that provide support beyond China's borders to its space operations.<sup>173</sup> In addition, it is reported that China operates overseas space telemetry tracking stations in Pakistan, Kiribati, Kenya, and Namibia.<sup>174</sup>

- China's large suite of satellites includes an extensive communications capability. These dual-use systems include Chinasat, APStar, Asiasat, and Sinosat. China maintains numerous satellites for imagery intelligence, remote sensing, synthetic aperture radar imagery, and oceanographic and environmental monitoring, including the Ziyuan, CBERS-2, Haiyin, Jianbing, and Huanjing series. China also has electronic and signals intelligence satellites. Its Compass<sup>175</sup> system is similar to the U.S. GPS system in that it provides positional data that enable China accurately to direct missiles against targets at extended ranges.<sup>176</sup> There currently are five Compass satellites operating over eastern China and the western Pacific Ocean with an additional 30 planned.<sup>177</sup>

- China recently has strengthened the integration of its dual-use space assets and PLA operations. This increasingly allows the military to meet its needs—including intelligence collection, force planning, military operations, and battle assessment—with the space architecture already in place. This system is secure, survivable, and interoperable down to the lowest levels of the PLA.<sup>178</sup>

- China has significant antisatellite capabilities. The capabilities go far beyond those demonstrated in the January 2007 "test" that destroyed an obsolete Chinese weather satellite. They include orbital direct attack weapons and directed energy weapons for dazzling or damaging satellites, both of which currently are under development.<sup>179</sup> China also is researching technology for electronic attack,<sup>180</sup> such as jamming, against an adversary's space assets as well as its ground support networks.<sup>181</sup> Some Chinese authors think that "battlefield situational awareness" is so critical to modern combat operations that China must be able and ready to "destroy or jam" an adversary's situational awareness systems.<sup>182</sup>

### ***The Management Structure for China's Space Programs***

Kevin Pollpeter from the Defense Group Incorporated writes:

*China's space program is inherently military in nature. While cooperation does exist between NASA [the National Air and Space Administration] and the U.S. military, the Chinese space program lacks the bureaucratic walls which make NASA a predominantly civilian organization in both focus and culture. Indeed, China's space program is a military-civilian joint venture in which the military develops and operates its satellites and runs its infrastructure, including China's launch sites and satellite operations center. The China National Space Administration, often incorrectly referred to as China's NASA, mainly functions as a civilian front for international cooperation and as a liaison between the military and defense industry. In fact, the China National Space Administration does not even manage [some] important space cooperative activities. . . .<sup>183</sup>*

China does not distinguish between a military space program and a civilian program. The People's Liberation Army operates China's satellites as well as all terrestrial launch and support facilities. This structure ensures the primacy of military interests, while it seeks to integrate the civilian applications.<sup>184</sup> Peng Qiang, a senior manager for China's lunar mission, when meeting with visitors from a U.S. think tank, refused even to discuss the operation of China's space control center, "because it is run by the military."<sup>185</sup>

### ***The Key Military Objectives of China's Space Program***

According to Jing-dong Yuan, a professor at the Center for Non-proliferation Studies at the Monterey Institute of International Studies, China has concluded that space is an essential arena for future warfare and is important not only for improving intelligence gathering but also for enhancing command and control of combat forces. Previously, China opposed any military use of space.<sup>186</sup> However, in 2002 the government shifted its position and limited its opposition to weapons in space.<sup>187</sup> Changing directions again in its 2006 Defense White Paper, China completely omitted any indication of opposition to military equipment or weapons in space.<sup>188</sup> There continue to be discrepancies in China's public statements and actions on this topic. In September 2008, a PLA general and current director of the government-related think tank the Chinese Institute for International Security Studies, Xiong Guangkai, stated that China firmly opposes the militarization of space.<sup>189</sup> This is despite the fact that China tested an antisatellite weapon in 2007 and continues to put military-related satellites in space.

In February 2008, China entered the space militarization debate again by jointly sponsoring with Russia a proposed treaty at the United Nations (UN) Conference on Disarmament that prohibits "the placement of weapons in outer space" and the "use of force against outer space objects."<sup>190</sup> But China's rhetorical stance favoring only peaceful uses of space has not limited its work to harness space for military advantage. In the near term, China's military space program aims to counter U.S. capability asymmetrically in order to reduce the advantage the United States enjoys from the

quantity and superior capabilities of its weapons and the quality of its combat forces. China is focusing its space efforts on developing capabilities that target potential strategic vulnerabilities of the United States. During the period from 2006 to 2020, China aims to build comprehensive national power that includes not only military strength but also economic strength and diplomatic influence.<sup>191</sup> (For additional discussion see chap. 2, sec. 2, “China’s Views of Sovereignty and Methods of Controlling Access to its Territory.”)

The People’s Liberation Army characterizes its strategy in broad terms as an active defense.<sup>192</sup> However, as PLA strategist Chen Zhou explained in a Communist Party publication in March 2008, China must “pay great attention to carrying out offensive activities aggressively and organizing preemptive strikes.”<sup>193</sup> Practically speaking, the strategy not only has defensive elements but also has many that are offensive in nature—which Chinese officers sometimes acknowledge. With reference to space, China could use laser technology to blind temporarily a U.S. reconnaissance satellite operating over international waters. This action could be viewed by many as purely defensive. However, China also could use its ASAT capability to destroy a U.S. satellite operating over its territory. While the immediate goal is the same, many who might be willing to characterize blinding as defensive would regard destruction as offensive.<sup>194</sup> The offensive attributes of China’s strategy are a cause of concern to the United States.

In addition to its existing space program, China plans to continue aggressively developing a wide array of space and counter-space capabilities.<sup>195</sup> Its space plans include the following:

- Launching 15 rockets and 17 satellites in 2008.<sup>196</sup>
- Developing a new line of rocket engines that will provide China with heavy lift capability similar to the U.S. Air Force Evolved Expendable Launch Vehicle.<sup>197</sup> This line is scheduled to become operational in 2010 and is required for heavier payloads such as space station modules or larger satellites.<sup>198</sup>
- Performing in-orbit docking of two orbital modules. This capability is required in order to construct and operate a manned space station.<sup>199</sup>
- Developing a small lunar rover by 2015. A successful lunar rover mission may lead to a successful lunar sample mission providing scientific insight into the composition of the lunar soil.<sup>200</sup>
- Implementing a high-resolution Earth observation system.<sup>201</sup> Satellite photographs have a wide variety of military and civilian uses, and increased resolution will improve the utility of this capability.
- Developing ground relay stations for remote-sensing satellites.<sup>202</sup> These stations will allow increased access to satellite information, enabling their data to be available for greater periods, even in some cases after satellites move over the horizon.
- Improving the Compass navigation satellite system.<sup>203</sup> This system will use a much larger number of nonstationary satellites than China currently is employing for this purpose and aims for worldwide coverage.

- Launching geostationary orbit telecommunications satellites.<sup>204</sup> Each of these satellites will provide uninterrupted communications for users in the portion of the globe covered by its “footprint.”

### ***The Impact of China’s Space Program on U.S. Security***

The potential effect of China’s space program on U.S. national security is significant. First, it is steadily increasing the vulnerability of U.S. assets. Improvements in its imagery and intelligence satellites will enable China to locate U.S. assets such as carrier battle groups more accurately and rapidly and from greater distances. Improved communications satellites will enable China to pass important targeting information more quickly and securely to guided missiles or other weapon systems. Improved GPS-type navigational and weather satellites will enable missiles to fly more accurately to their targets. Finally, the cycle is completed by the battle damage assessment that imagery and intelligence satellites provide to Chinese commanders as weapon systems engage their targets.<sup>205</sup>

Many U.S. weapon systems and deployed military forces depend on space support for targeting, navigational, and communications support. A large portion of the U.S. space systems’ architecture consists of ground-based nodes and centers located around the United States and the globe far from the battlefield.

The ground nodes and centers in space or on the ground are critical elements of U.S. military power. As such, they are potential targets for China. Some Chinese strategists believe that space-related installations, including ground stations, are so critical that they are valid targets during a conflict.<sup>206</sup> China could choose to engage these critical assets physically with missiles or nonkinetically through means such as a computer network attack.<sup>207</sup>

China’s growing reliance on space for military purposes increases the likelihood that any future conflict between China and the United States will involve actions directed against each other’s space systems’ assets. These offensive and defensive actions may be directed against either assets.

### **China’s Cyber Operations Program**

U.S. computer security authorities detected a series of cyber intrusions in 2002 into unclassified U.S. military, government, and government contractor Web sites and computer systems. This large-scale operation, code named Titan Rain by the U.S. government, was attributed to China.<sup>208</sup> Targeted locations included the U.S. Army Information Systems Engineering Command, the Naval Ocean Systems Center, the Missile Defense Agency, and Sandia National Laboratories. Major General William Lord from the U.S. Air Force Office of Warfighting Integration, speaking at an information technology conference, said that China downloaded 10 to 20 terabytes of data.<sup>209</sup> For comparison, the entire print collection of the Library of Congress contains approximately 10 terabytes of data. In addition to seeking to acquire important information about military and government activities, the operation conducted reconnaissance of the U.S. command and control system, gaining infor-

mation that could be used for future targeting. The U.S. Strategic Command reported that in 2007, the Department of Defense estimated that five million computers experienced 43,880 incidents of malicious activity from all sources—a 31 percent increase over the previous year.<sup>210</sup>

#### **TYPES OF COMPUTER NETWORK OPERATIONS**<sup>211</sup>

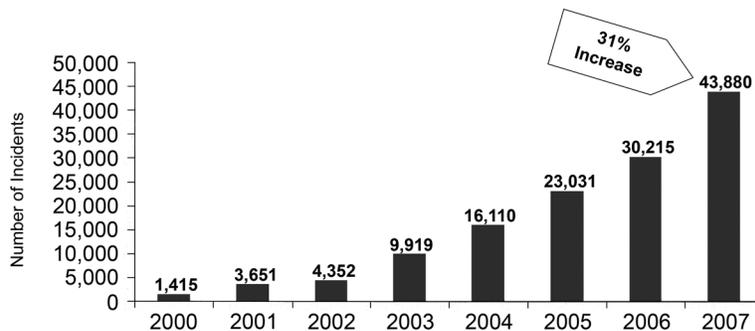
*Computer Network Operations (CNO):* Comprised of computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations.

*Computer Network Attack (CNA):* Actions taken via computer networks to disrupt, deny, degrade, or destroy information residing in computers and computer networks, or the computers and networks themselves.

*Computer Network Defense (CND):* Actions to protect information systems and computer networks, and to monitor for, analyze, detect, and respond to unauthorized activity within those networks.

*Computer Network Exploitation (CNE):* Actions to gather data from target information systems or networks or map target networks for future CNA operations.

**U.S. Department of Defense (DoD) Reported Incidents of Malicious Cyber Activity**



Source: U.S.-China Economic and Security Review Commission, Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities, testimony of Colonel Gary McAlum, Washington, DC, May 20, 2008.

#### ***China's Incorporation of Cyber Operations into its Warfare Arsenal***

Colonel Gary McAlum, chief of staff for the U.S. Strategic Command's Joint Task Force for Global Network Operations, testified to the Commission that China has recognized the importance of cyber operations as a tool of warfare, as demonstrated by the increased resources and training it is focusing on cyber operations. The training addresses both cyber attacks and cyber intrusions. Colonel McAlum said that China currently has the intent and capa-

bility to conduct cyber operations anywhere in the world at any time. China has an active cyber espionage program. Since China's current cyber operations capability is so advanced, it can engage in forms of cyber warfare so sophisticated that the United States may be unable to counteract or even detect the efforts.<sup>212</sup>

By some estimates, there are 250 hacker groups in China that are tolerated and may even be encouraged by the government to enter and disrupt computer networks.<sup>213</sup> The Chinese government closely monitors Internet activities and is likely aware of the hackers' activities. While the exact number may never be known, these estimates suggest that the Chinese government devotes a tremendous amount of human resources to cyber activity for government purposes. Many individuals are being trained in cyber operations at Chinese military academies,<sup>214</sup> which does fit with the Chinese military's overall strategy, according to the U.S. Department of Defense's *2008 Annual Report to Congress: Military Power of the People's Republic of China*.<sup>215</sup>

Other nations are concerned about the level, sophistication, and orientation of China's cyber operations. During the Commission's visit to Japan in August 2008, a representative of the Ministry of Defense told Commissioners that the ministry's newest white paper to be released in September 2008 would discuss outer space and cyber space as areas in which China has "great interest" (and the white paper did so).<sup>216</sup> During that same Commission trip, Taiwan's Defense Minister Chen Chao-min acknowledged that Taiwan anticipated a potent cyber attack, were it to become involved in an open conflict with China, and told Commissioners that he had established a special task force to examine the issue and recommend steps Taiwan could take to reduce its cyber vulnerability.

According to Tim Thomas, an expert on People's Republic of China (PRC) cyber operations from the U.S. Army's Fort Leavenworth Foreign Military Studies Office, cyber operations have several appealing characteristics from a military viewpoint. The first is that the warning time for an attack, and the time frame for defensive response, is extremely limited. Cyber attacks travel at the speed of light and require little physical preparation. A second appeal is the lack of attribution. Cyber operations can take a layered and circuitous route to the target, so that only the last computer utilized in the series can be identified. Therefore, the victim's ability to retaliate accurately is hindered or eliminated. A third appeal is that cyber operations can confuse and frustrate the target nation. Cyber attacks can target power grids, financial systems, and other critical infrastructure, rendering them inoperable, thereby constituting the same effect as a kinetic attack (a traditional military strike using physical force). However, even if the culprit can be reliably identified (which is difficult to accomplish), the target nation may lack an effective means to mount a cyber counter-attack. Retaliating kinetically may be seen by both the nation against which a retaliatory strike is executed and, importantly, by other nations and multilateral organizations as both unjustified and escalatory.<sup>217</sup> One reason this may be viewed as unjustified is because there is no clear consensus on when a cyber attack constitutes an act of war.

### ***Vulnerable U.S. Cyber Infrastructure***

Private sector networks in the United States, networks operated by civilian U.S. government agencies, and unclassified U.S. military and intelligence agency networks increasingly are experiencing cyber intrusions and attacks. Although classified military and intelligence networks are designed to be protected by insulation from the Internet, networks connected to the Internet are vulnerable even if protected with hardware and software firewalls and other security mechanisms. The government, military, businesses and economic institutions, key infrastructure elements, and the population at large of the United States are completely dependent on the Internet. Internet-connected networks operate the national electric grid and distribution systems for fuel. Municipal water treatment and waste treatment facilities are controlled through such systems. Other critical networks include the air traffic control system, the system linking the nation's financial institutions, and the payment systems for Social Security and other government assistance on which many individuals and the overall economy depend. A successful attack on these Internet-connected networks could paralyze the United States.

China is targeting U.S. government and commercial computers for espionage. Alan Paller from the SANS Institute, an Internet security company, believes that in 2007 the 10 most prominent U.S. defense contractors, including Raytheon, Lockheed Martin, Boeing, and Northrop Grumman, were victims of cyber espionage through penetrations of their unclassified networks.<sup>218</sup> In 2005 hackers from China exfiltrated a stockpile of files on the National Aeronautics and Space Administration (NASA) Mars Reconnaissance Orbiter, including files on the propulsion system, solar panels, and fuel tanks. In the same year, the aviation mission planning system for army helicopters and flight planning software used by the army and air force were stolen from the Army Aviation and Missile Command at Redstone Arsenal, Alabama.<sup>219</sup>

An excellent example of the problem the United States faces is the unclassified U.S. military network called the NIPRNet (Non-secure Internet Protocol Router Network). This network is the most vulnerable military network.<sup>220</sup> (It is separate from the SIPRNet [Secret Internet Protocol Router Network] that carries classified information.) Despite the fact it is an unclassified system, the NIPRNet is crucial to the effective operation of the U.S. military, during both peace and war. The traffic it carries includes all DoD bill payments; the daily calendars for admirals and generals; troop and cargo movements; aircraft locations and movements; aerial refueling missions; medical records for military personnel and their dependents; soldier and officer evaluation reports; unit deployment information; and all e-mails among Department of Defense and military personal digital assistant communications devices.

The NIPRNet is vulnerable because it connects to the World Wide Web. While these connections allow it to access the Internet, they also provide an opportunity for unauthorized intrusions. Intrusions could have a variety of nefarious purposes, including stealing sensitive information or planting viruses or other malware that could be activated during a time of crisis and cripple the systems into which they had been inserted. There currently are 17 connec-

tions between the NIPRNet and the Internet. DoD is decreasing that number to simplify monitoring and security procedures. However, DoD is so dependent on the functions that cross the NIPRNet that it also must take into account the risk of providing too few portals. The risk is that vital functions could not be carried out if several portals became inoperable.<sup>221</sup>

China can access the NIPRNet<sup>222</sup> and views it as a significant Achilles' heel and as an important target of its asymmetric capability.<sup>223</sup> The ability to manipulate or disable the NIPRNet, or to use it to disable discrete, defense-related functions that depend on it, gives China the potential capability to delay or disrupt U.S. forces without physically engaging them—and in ways it lacks the capability to do conventionally.<sup>224</sup>

In the past two decades, China has observed how the U.S. military has operated successfully overseas and also has noted that the United States in many cases utilizes a deployment or buildup phase. Examples include the first Gulf War, Kosovo, and Operation Iraqi Freedom. Due to the great distances in the Pacific area of operations, were the United States to think a conflict near China was probable, the U.S. military would begin its preparations with a deployment or buildup phase. China is depending on this and believes that, by cyber attacking U.S. logistics functions in the early buildup stages of a conflict, it can delay or disrupt U.S. forces moving to the theater.<sup>225</sup> This conceivably could alter the course of a conflict over Taiwan. China views Taiwan's will to fight as the key to success, and Chinese authors postulate that successfully delaying a U.S. response after a hard and fast strike against Taiwan will create a window of opportunity in which it may be possible to force Taiwan to capitulate.<sup>226</sup>

In operationalizing this cyber strategy, authors of China's military doctrine have articulated five key elements. These elements are the following:<sup>227</sup>

- Defense. Many Chinese authors believe the United States already is carrying out offensive cyber espionage and exploitation against China. China therefore must protect its own assets first in order to preserve the capability to go on the offensive.
- Early use. PLA analysts believe that in many cases a vulnerable U.S. system could be unplugged in anticipation of a cyber attack. Therefore, for an attack to be truly effective, it must be launched early in a conflict before the adversary has time fully to protect itself.
- Information operations. Cyber operations can be used to manipulate an adversary's perception of the crisis, such as by planting misinformation. This could obviate the need for a conventional confrontation or advantageously shape an adversary's response.
- Attacking an enemy's weaknesses. China's strategists believe the United States is dependent on information technology and that this dependency constitutes an exploitable weakness.
- Preemption. Many PLA strategists believe there is a first mover advantage in both conventional and cyber operations against the United States. Therefore, in order to succeed, they should strike first.

The global supply chain for telecommunications items introduces another vulnerability to U.S. computers and networks. Components in these computers and networks are manufactured overseas—many of them in China. At least in theory, this equipment is vulnerable to tampering by Chinese security services, such as implanting malicious code that could be remotely activated on command and place U.S. systems or the data they contain at risk of destruction or manipulation. In a recent incident, hundreds of counterfeit routers made in China were discovered being used throughout the Department of Defense.<sup>228</sup> This suggests that at least in part, Defense Department computer systems and networks may be vulnerable to malicious action that could destroy or manipulate information they contain.

### Conclusions

- China continues to make significant progress in developing space capabilities, many of which easily translate to enhanced military capacity. In China, the military runs the space program, and there is no separate, distinguishable civilian program. Although some Chinese space programs have no explicit military intent, many space systems—such as communications, navigation, meteorological, and imagery systems—are dual use in nature.
- The People’s Liberation Army currently has sufficient capability to meet many of its space goals. Planned expansions in electronic and signals intelligence, facilitated in part by new, space-based assets, will provide greatly increased intelligence and targeting capability. These advances will result in an increased threat to U.S. military assets and personnel.
- China’s space architecture contributes to its military’s command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capability. This increased capability allows China to project its limited military power in the western and southern Pacific Ocean and to place U.S. forces at risk sooner in any conflict.
- Cyber space is a critical vulnerability of the U.S. government and economy, since both depend heavily on the use of computers and their connection to the Internet. The dependence on the Internet makes computers and information stored on those computers vulnerable.
- China is likely to take advantage of the U.S. dependence on cyber space for four significant reasons. First, the costs of cyber operations are low in comparison with traditional espionage or military activities. Second, determining the origin of cyber operations and attributing them to the Chinese government or any other operator is difficult. Therefore, the United States would be hindered in responding conventionally to such an attack. Third, cyber attacks can confuse the enemy. Fourth, there is an underdeveloped legal framework to guide responses.
- China is aggressively pursuing cyber warfare capabilities that may provide it with an asymmetric advantage against the United States. In a conflict situation, this advantage would reduce current U.S. conventional military dominance.