

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now](#)

TECHNOLOGY

Cisco Poised to Help China Keep an Eye on Its Citizens

By LORETTA CHAO in Beijing and DON CLARK in San Francisco

July 5, 2011

Cameras in Beijing's Tiananmen Square. U.S. firms can sell surveillance gear in China, but not equipment that is used only for crime control. *Getty Images*

Western companies including Cisco Systems Inc. are poised to help build an ambitious new surveillance project in China—a citywide network of as many as 500,000 cameras that officials say will prevent crime but that human-rights advocates warn could target political dissent.

The system, being built in the city of Chongqing over the next two to three years, is among the largest and most sophisticated video-surveillance projects of its kind in China, and perhaps the world. Dubbed "Peaceful Chongqing," it is planned to cover a half-million intersections, neighborhoods and parks over nearly 400 square miles, an area more than 25% larger than New York City.



Cisco Systems and other companies are poised to help build an ambitious new surveillance project in China, a citywide network of cameras that could prevent crime but that human-rights advocates say could target political dissent. Don Clark reports on digits.

The project sheds light on how Western tech companies sell their wares in China, the Middle East and other places where there is potential for the gear to be used for political purposes and not just safety. The products range from Internet-censoring software to sophisticated networking gear. China in particular has drawn criticism for treating political dissent as a crime and has a track record of using technology to suppress it.

An examination of the Peaceful Chongqing project by The Wall Street Journal shows Cisco is expected to supply networking equipment that is essential to operating large and complicated surveillance systems, according to people

familiar with the deal.

The U.S. has prohibited export of crime-control products to China (for instance, fingerprinting equipment) ever since Beijing's deadly 1989 Tiananmen Square crackdown. But the U.S. restrictions don't prohibit sale of technologies such as cameras that can be used in many ways—to tame, say, either traffic jams or democracy marches. This loophole troubles some critics. There is no indication that Cisco is selling

products customized for crime control.

Journal Community >

Western companies' pursuit of sales in China underscores a fundamental question for businesses and policy makers alike: Should companies be held accountable if foreign governments use their products for political suppression?

Cisco was brought in to the Chongqing project by Chinese security company Hikvision Digital Technology Co., the project's main contractor, Hikvision officials and others say. It is unclear whether Cisco's participation has been finalized, although one person familiar with the matter says it is close.

Officials at Cisco, based in San Jose, Calif., declined to discuss its possible involvement in detail. A company spokesman stressed that Cisco "hasn't sold video cameras or video-surveillance solutions in any of our public infrastructure projects in China."

More

[China Real Time: Are Firms Responsible for How Their Products Are Used?](#)

[Cisco Faces Lawsuits, Criticism Over Past China Activities](#)

The company has previously said—including in a June blog post by Cisco's general counsel, Mark Chandler—that the company strictly abides by the Tiananmen export controls and doesn't supply any gear to China that is "customized in any way" to facilitate repressive uses.

Cisco is the world's biggest maker of networking equipment, which includes routing and switching systems that send data between computers and connect systems to the Internet. The company has stirred controversy in the past for its China dealings.

The Chongqing project is also attracting interest from other U.S. companies, including Alabama software maker Intergraph Corp. Hewlett-Packard Co. also expects to bid on part of the project, according to a senior H-P executive.

The people familiar with the matter said H-P may be looking to supply servers or storage equipment for Peaceful Chongqing.

Asked about concerns about political use of the system, Todd Bradley, an executive vice president who oversees H-P's China strategy, said in an interview last week in China, "We take them at their word as to the usage." He added, "It's not my job to really understand what they're going to use it for. Our job is to respond to the bid that they've made."

Censorship Inc. >

[Mideast Uses Western Tools to Battle the Skype Rebellion](#) 6/1/2011

[Iran Vows to Unplug Internet](#) 5/28/2011

[U.S. Products Help Block Mideast Web](#) 3/28/2011

Another possible participant in the Chongqing project is Intergraph, a Huntsville, Ala., company that made a bid through Cisco to provide customized software for the effort, said Bob Scott, head of Intergraph's security group. It is unclear if the company, a unit of Sweden's Hexagon AB, will ultimately be hired.

Although sale of surveillance technology to repressive nations is permissible, some critics have harsh words for companies that do so. "The business community is only hearing what it wants to hear and disregarding the rest," said Rep. Frank Wolf, a Virginia Republican who co-chairs the Tom Lantos Human Rights Commission, a nonpartisan rights group made up of members of Congress.

Chongqing, a sprawling metropolis in southwestern China, is one of the most populous cities in the nation with an urban population of at least 12 million. The hillside Yangtze River port, famous for spicy hot-pot and often covered in fog, was China's capital from 1938 to 1945. Today, it is being developed as a gateway to the country's western hinterland.

Chongqing has gained prominence the past two years because of its Communist Party chief, [Bo Xilai](#), a rising political star who has led a controversial crackdown on organized crime that some lawyers have criticized for what they say are violations of legal due process.

Mr. Bo declined to comment. He is expected to become one of China's top leaders next year by being appointed to China's Politburo Standing Committee, the nation's top decision-making body.

Chongqing's government has said it plans to invest more than \$800 million of its own in building the Peaceful Chongqing system. Another \$1.6 billion is coming from other, unspecified sources, the city has said. Hikvision's president, Hu Yangzhong, said in an interview that government funds would go toward building the central surveillance network and installing a portion of the cameras, while more cameras

Chongqing's party chief, Bo Xilai, led a controversial crime crackdown. *Getty Images*

would be installed by owners of residences, office buildings and others—all of which would be linked to the network.

Video-surveillance systems can serve many purposes and are routinely used for benign purposes by cities world-wide to fight crime and ease traffic. Still, civil libertarians raise concerns including in the U.S. that the technology can invade privacy and is poorly regulated.

Human-rights advocates say Chinese police have used surveillance footage to identify people in political protests. Jailed Chinese artist-activist Ai Weiwei, who was released last month, complained before he was apprehended on April 3 that police were using cameras to monitor him.

Corinna-Barbara Francis, a researcher at Amnesty International, said surveillance footage has been used to identify and apprehend peaceful protesters in China, including in Xinjiang and Tibet. "In China there's ample evidence that they use" video surveillance "to crack down and then criminalize activity which should not be criminalized," Ms. Francis said.

The Chongqing government declined to comment, as did China's Ministry of Public Security and the State Council Information Office. Chinese leaders have long argued that maintaining social stability and economic growth takes precedence over political rights.

Hikvision's president, Mr. Hu, said he believes the project's goal is to cut crime, not target political dissidents. "China has a very

serious public-security problem," he said in an interview last week. He blamed an epidemic of robbery and other crimes on the flood of poor migrants into China's cities and a growing wealth gap.

Mr. Hu said Chongqing's new surveillance system will be tied in to an information network that Cisco is already building in the city, where Cisco has announced a high-profile alliance under a program it calls Smart+Connected Communities—an initiative under which Cisco consults with governments around the world to use technology to tackle civic problems such as transportation,

healthcare and education.

According to the Chongqing government's website, Cisco Chief Executive John Chambers told the city's mayor in a meeting last year that he hoped the Smart+Connected project could create a "model in Chongqing which can be popularized in China."

Executives at Western companies say they must weigh the possibility that technology could be misused against the business risks of missing out on a lucrative market. "We do have concerns," said Intergraph's Mr. Scott. "On the other hand, we want to do business there," he said, noting that the company's software is also used for environmental and other projects in China.

"We're just the technology platform," he said, adding that it is the responsibility of the buyers "to meet and adhere to laws and policies" of their jurisdictions. Ultimately, Intergraph has "to manage the risk against the gain."

In an April interview with the Journal, Bill Stuntz, general manager of Cisco's physical-security business, said Cisco gives careful consideration to how its products are used in China and doesn't want them to be used for repressive purposes. He declined to discuss specific projects in China but noted that sales of security equipment there have been expanding rapidly. He said Cisco is providing products that include networking equipment and servers along with support for some large video-surveillance systems, though not video cameras.

China has become the fastest growing market for surveillance equipment, although it isn't yet the biggest, according to IMS Research, a U.K. firm that studies the market. The surveillance markets in the U.S. and Europe are growing at single-digit rates while surveillance-related revenue in China is growing at 23% a year. Surveillance-equipment sales alone, not including networking gear or software, totaled \$1.7 billion last year.

Chongqing's government says on its website that its current surveillance system is outdated, allowing police to directly tap into just 15,000 of the total 300,000 cameras. It wants the new system to be among the world's most advanced.

Mr. Scott of Intergraph says Chongqing wants not only to increase camera count, but also to have video managed and delivered to dozens of police precincts and other organizations. The project presents challenges "that have not really been done anywhere else in the world," he said.

Mr. Scott said his company spent three years developing software that enables multiple agencies to control cameras and also analyzes video feeds for unusual situations like fires or the formation of crowds.

The number of surveillance cameras in Chinese cities including Chongqing appears to dwarf that of other cities around the world, though comparisons are tough because cities generally don't disclose their camera counts.

A 2008 report by the state-run Xinhua news agency said Beijing had some 280,000 cameras in its system. By comparison, privacy advocates in the U.S., including the American Civil Liberties Union, estimate Chicago has 10,000 cameras. The New York Civil Liberties Union estimated in 2009 that there were 8,000 cameras in New York.

—Kersten Zhang, Yoli Zhang, Jason Dean and Cari Tuna contributed to this article.

Write to Loretta Chao at loretta.chao@wsj.com and Don Clark at don.clark@wsj.com

Copyright 2013 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com