In China, business travelers take extreme precautions to avoid cyber-espionage

By Ellen Nakashima and William Wan, Published: September 26

Packing for business in China? Bring your passport and business cards, but maybe not that laptop loaded with contacts and corporate memos.

China’s massive market beckons to American businesses — the nation is the United States’ second-largest trading partner — but many are increasingly concerned about working amid electronic surveillance that is sophisticated and pervasive.

Security experts also warn about Russia, Israel and even France, which in the 1990s reportedly bugged first-class airplane cabins to capture business travelers’ conversations. Many other countries, including the United States, spy on one another for national security purposes.

But China’s brazen use of cyber-espionage stands out because the focus is often corporate, part of a broader government strategy to help develop the country’s economy, according to experts who advise American businesses and government agencies.

“I’ve been told that if you use an iPhone or BlackBerry, everything on it — contacts, calendar, e-mails — can be downloaded in a second. All it takes is someone sitting near you on a subway waiting for you to turn it on, and they’ve got it,” said Kenneth Lieberthal, a former senior White House official for Asia who is at the Brookings Institution.

Chinese government officials say cyber-spying is a problem in much of the world. “It’s advisable for all international travelers to take due precautions with their computers and cellphones,” embassy spokesman Wang Baodong said. “China is not less insecure than other countries.”

Some industrial cyber-espionage takes place in the U.S corporate world, experts say, but not nearly to the extent found in China. Also, the U.S. government reportedly does not conduct economic espionage on behalf of U.S. industry.

Travelers there often tote disposable cellphones and loaner laptops stripped of sensitive data. Some U.S. officials take no electronic gear. And a few corporate executives detour to Australia rather than risk talking business in a bugged Chinese hotel room.
Other travelers hide files on thumb drives, which they carry at all times and use only on off-line computers. One security expert, who spoke on the condition of anonymity to avoid drawing scrutiny from the Chinese government, buys a new iPad for each visit, then never uses it again.

“It’s real easy for them [the Chinese] to read everything that goes in and out of the country because the government owns all the networks,” said Jody Westby, chief executive of Global Cyber Risk, a consulting firm.

“The real problem here is economic espionage,” she said. “There are countries where the search for economic information and high-value data is so aggressive that companies or people are very hesitant about taking their laptops to those countries.”

Business travelers began adopting such safety measures for China several years ago, experts say. On the eve of the 2008 Beijing Olympics, Joel Brenner, then the U.S. national counterintelligence executive, first issued government safety guidance to overseas travelers, with such tips as: “If you can do without the device, don’t take it.”

Though no country was named, “it was really directed at countries like China and Russia,” Brenner said in a recent interview.

He based his 2008 warning on cases in which Chinese malware was remotely inserted into cellphones; the malware then infected computer servers in the United States. He said the networks in every major hotel are monitored by Chinese security agencies.

“What’s at stake is not only the security of your current communications, but the security of your secrets back home,” said Brenner, who advises clients on data security at the law firm Cooley LLP. “That’s the real danger.”

When then-Commerce Secretary Carlos Gutierrez flew to Beijing for trade talks in December 2007, he left his laptop unattended, enabling Chinese agents to surreptitiously copy its contents, according to news reports.

Intrusions into computer networks also have been reported at the State, Commerce and Defense departments; they allegedly originated in China.

Not all spying is done by state agencies, said one consultant for U.S. manufacturers in China, who spoke on the condition of anonymity to avoid drawing attention to her firm. “A lot of it is business-to-business corporate espionage, but that gets complicated in a place like China, where so many companies are state-owned enterprises linked to the government,” she said.

Government travelers also take precautions in Russia. One former State Department official recalled that on a trip to Moscow last year, he and other officials left their BlackBerrys and laptops on their U.S. government airplane. They used special computers at their hotel and equipment “that we were confident could not be compromised by the Russians.”

The guidance security experts give travelers to high-risk countries is extensive: Assume any wireless device will be compromised. Change passwords regularly. Back up information. Do not accept thumb drives as gifts. Do not assume you’re too insignificant to be targeted.

Chicago-based corporate lawyer Thomas Gehl, for instance, takes an encrypted laptop to China and avoids detailed discussions of clients’ joint ventures on his cellphone.

Another common tactic is to remove batteries from cellphones, which makes digital tracking more difficult and prevents microphones from being activated remotely. The practice has become so routine that Western
In China, business travelers take extreme precautions to avoid cyber-espi...

In China, business travelers take extreme precautions to avoid cyber-espi...