the FEDERALIST

Be lovers of freedom and anxious for the fray.

China Is Going To Spy On Everyone At The Nuclear Summit In Singapore

John Daniel Davidson

June 12, 2018

Here's a tip for journalists covering the U.S.-North Korea nuclear summit in Singapore this week: if you get free media swag that plugs into your phone or computer, like a USB fan, don't use it. For that matter, you might want to take the batteries out of your smartphone, buy a "burner" phone, and never let any electronic devices out of your sight while you're covering the summit.

Why? Because China is going to be spying on you.

More than 3,000 journalists are now in Singapore to cover the summit, giving Beijing a target-rich environment for all manner of hacking, tracking, and surveilling. China doesn't have a seat at the negotiating table, but it will be listening in as best it can, using everything from free USB fans to advanced forensic devices that can circumvent some forms of disk encryption and extract information from mobile phones and computers.

Beijing Is Pulling Out All The Stops To Spy On The Summit

It's not just journalists who should be worried about Chinese espionage at the summit. American officials are anticipating that Beijing will target the entire U.S. delegation. According to a recent NBC News report, "Americans will sweep for bugs in rooms at the Capella Hotel that could be used for side discussions, and could erect tents inside hotel meeting rooms to block any concealed cameras from viewing classified documents."

Julian Sanchez, an expert on national security and intelligence surveillance at the Cato Institute, says China's efforts "are likely to include both traditional and relatively crude measures—recruiting waiters to listen in on restaurant conversations, or physically searching hotel rooms—as well as extremely sophisticated cyberattacks aimed at compromising smartphones and laptops or planting inconspicuous electronic listening devices."

In the past, those inconspicuous listening devices have been things like "friendship pins" the Chinese gave to the U.S. delegation during Trump's state visit with Xi Jinping last November, which members of the delegation were forbidden from wearing in secure areas because they likely contained listening devices.

During that visit, U.S. officials said their belongings were rifled through when they were away from their hotel rooms. According to NBC News, "Some senior members of Trump's delegation packed carry-on bags with anything they didn't want the Chinese to see and took the bags wherever they went, including out to dinner in restaurants."

Staff at the Capella Hotel in Singapore, which is hosting the summit, might also be suspect. In one recent case, a top U.S. official stationed in China repeatedly had trouble with malfunctioning key cards. When he brought one of them back to the United States, security officials found a microphone embedded in it.

As for members of the news media who haven't had much experience in dealing with Chinese surveillance—and haven't been briefed by counterintelligence experts—Sanchez says that almost anything can be bugged these days, and "at an absolute minimum, no reporter should be plugging government-provided USB devices into their laptops, though that's probably one of the less subtle types of attack they can expect."

China Has Waged a Cold War Against The U.S. For Years

All of this should be understood in the broader context of China's aggressive cyberespionage in recent years. The 2015 Office of Personnel Management hack was quite possibly the worse data breach in U.S. history, and it gave Beijing access to sensitive information about tens of millions of Americans employed by the federal government.

That probably includes people like Ron Hansen, a former Defense Intelligence Agency case officer who was arrested in Seattle last week and charged with attempted espionage. Hansen, a fluent Mandarin speaker, was deeply in debt and had allegedly received $800,000 in "funds originating from China" since 2013.

Kevin Mallory, a former U.S. intelligence officer who also speaks fluent Mandarin and is also deeply in debt, is on trial for espionage, charged with attempting to pass classified information to the Chinese and smuggling technology to them.

In May, former CIA officer Jerry Chun Shing Lee was indicted on a conspiracy to commit espionage after a years-long CIA mole hunt that began when the agency began to lose informants in China in 2012. Experts believe Beijing is using the intelligence gleaned from the OPM hack to target Americans who have security clearances and are in financial trouble.

That would of course make perfect sense. China's military has a massive (100,000 strong) cyberespionage division, whose fingerprints have been on some of the largest attacks in recent history, like the 2015 attack on health insurer Anthem Blue Cross, which exposed sensitive data on as many 80 million Americans—names, Social Security numbers, birth dates, addresses, incomes.

Espionage At the Summit Is Only Part Of the Picture

China is not going to just sit back and let the nuclear summit in Singapore play out behind closed doors. Kim Jong-Un's regime is essentially a client of Beijing, relying on China for trade, aid, and energy. As if to underscore that point, Kim arrived in Singapore in an Air China jet.

“The Air China jet was one of three in a mini-armada that flew the North Korean entourage to Singapore,” reports *The New York Times*. “The other two were Russian-built aircraft operated by North Korea’s national carrier, Air Koryo.”

The *Times* quotes a Chinese aerospace columnist who noted that Kim’s flight to Singapore took an unusual route through Chinese airspace, indicating that the plane was likely escorted by Chinese fighter jets.

The nuclear summit and future of U.S.-North Korea relations is enormously important to China—one piece of a sweeping strategy to assert itself as a rival superpower to the United States and a regional hegemon in the Asia Pacific. Any deal Kim brokers with Trump will have to get Beijing’s approval. More than that, Beijing will be like a silent third party in the ensuing negotiations.

As for the summit itself, Sanchez warns that Chinese surveillance is not necessarily limited to time spent in Singapore: “A device implanted with malware could enable continuous surveillance even after reporters and delegates have returned to the United States or, more prosaically, credentials stolen from these devices could be used for prolonged monitoring of the associated accounts.”