Huawei connects rural America. Could it threaten the country's most sensitive military sites?

By Alex Marquardt and Michael Conte | March 11, 2019

(CNN) Outside Malmstrom Air Force Base in central Montana, spread across 13,800 square miles of open plains, more than 100 intercontinental ballistic missiles stand at the ready, buried deep underground in missile silos. These Minuteman III rockets are capable of delivering nuclear warheads at least 6,000 miles away and are part of the U.S. Strategic Command, which oversees the country's nuclear and missile arsenal.

A Triangle Communication cell phone tower near Moore, MT

Nestled among these silos are clusters of cell phone towers operated by a small rural wireless carrier. According to FCC filings, those cell towers use Chinese technology that security experts warn could allow China to gather intelligence while also potentially mounting network attacks in the areas surrounding this and other sensitive military installations.

Huawei, the Chinese company that makes the tower technology, is shunned by the major US wireless carriers (including AT&T, which owns CNN parent company WarnerMedia) and the federal government over national security concerns. Yet its technology is widely deployed by a number of small, federally-subsidized wireless carriers that buy cheaper Chinese-made hardware to place atop their cell towers. In some cases those cellular networks provide exclusive coverage to rural areas close to US military bases.

In congressional testimony last year, the heads of six major US intelligence agencies -- including the FBI and CIA - warned Americans against using Huawei devices and products. Security experts say that having its technology deployed so close to the nation's arsenal of ICBMs could pose a far greater threat.

"We know the Chinese are engaged in a massive espionage campaign against the US," said James Lewis, director of the Technology Policy Program at the DC-based think tank The Center for Strategic and International Studies. "We know that the Chinese engage in massive surveillance against their own population. You put two and two together and say, how comfortable do I feel having Huawei on the phone systems around my most important military bases?

Potential threats

Huawei is engaged in a pitched battle with the US government. The company is banned from bidding on US government contracts, and federal employees are forbidden from using its products. On March 7, Huawei sued the US government, arguing the ban is unconstitutional.

Huawei has extensive US and international operations and has vowed that it would never install or allow others to install so-called 'backdoors' into its equipment.

But experts fear the company, whose founder and CEO served in the Chinese military, could be susceptible to influence from Beijing. If China chooses to weaponize Huawei's radio transmitters and receivers placed on towers in sensitive areas, there's a long list of possible scenarios and types of information they could glean. Even if the military installations themselves aren't vulnerable, personnel working on or around them could be.

"It's a way to suck in data and carry out ISR (Intelligence, Surveillance and Reconnaissance)," says a former senior Pentagon information security official. "It's quite intrusive actually. I have no evidence [the Chinese] are doing it. But the potential, the opportunity, wow."

"What the overall status of the missile fields are, which are active, which are in maintenance status," he continued, "it may seem like innocuous data but this is a big deal."

A weaponized cell tower could shut down service, send out malign text messages and launch a denial of service attack, security experts tell CNN.

"The Chinese could decide to interfere with ICBM command and control, or with ICBM personnel, the people manning the missile silos," said Lewis from CSIS. "That's not a risk that you can dismiss. You have to say, it's a new strategic capability for China. Not one we expected. It's not military. It's not a weapon. It's not your traditional attack."

As scary as it sounds, Lewis admits it's unlikely that an outside radio transmitter would be able to penetrate the closed encrypted systems that control the missile installations.

"ICBMs are supposed to be pretty hard. That might not be easy to do," said Lewis, a former Foreign Service officer who was an adviser to the military. "But that doesn't mean our opponents won't try and figure out if they can do it."

Lewis points to a national intelligence law China passed in 2017 that gives the government sweeping powers under the pretext of national security. "If they ask Huawei, turn off the phones, tell us what people are doing, scramble the data going over it, block calls, make random phone calls, there's nothing we could really do to stop that," said Lewis.

Huawei says that law doesn't apply to telecom equipment providers that operate outside China, such as itself. "It doesn't allow the Chinese government to willy nilly put backdoors in products," said Andy Purdy, chief security officer for Huawei in the US.

In addressing the broader concerns, Purdy pointed to the extensive security measures they take to safeguard their clients' system. "Huawei does not operate or maintain the equipment and networks of our customers," said Purdy, while allowing that, "Nearly all networks and systems around the world are subject to penetration efforts, sometimes successfully, by sophisticated, well-resourced malicious actors such as a nation state." Still, to some, having any Huawei technology operating in the US is too much.

"It would be great if there wasn't a shred of Huawei anywhere in the United States," said Marcus Sachs, the former vice president for National Security Policy at Verizon who also served on the Defense Department's Joint Task Force for Computer Network Defense. He said the use of Huawei presents "critical national security implications."

"In theory, any piece of equipment could have the capability to do 'man in the middle.' It will know about every call placed, track all the internet traffic, what's going where," Sachs said. "The unencrypted information would be intercepted and sent back to China."

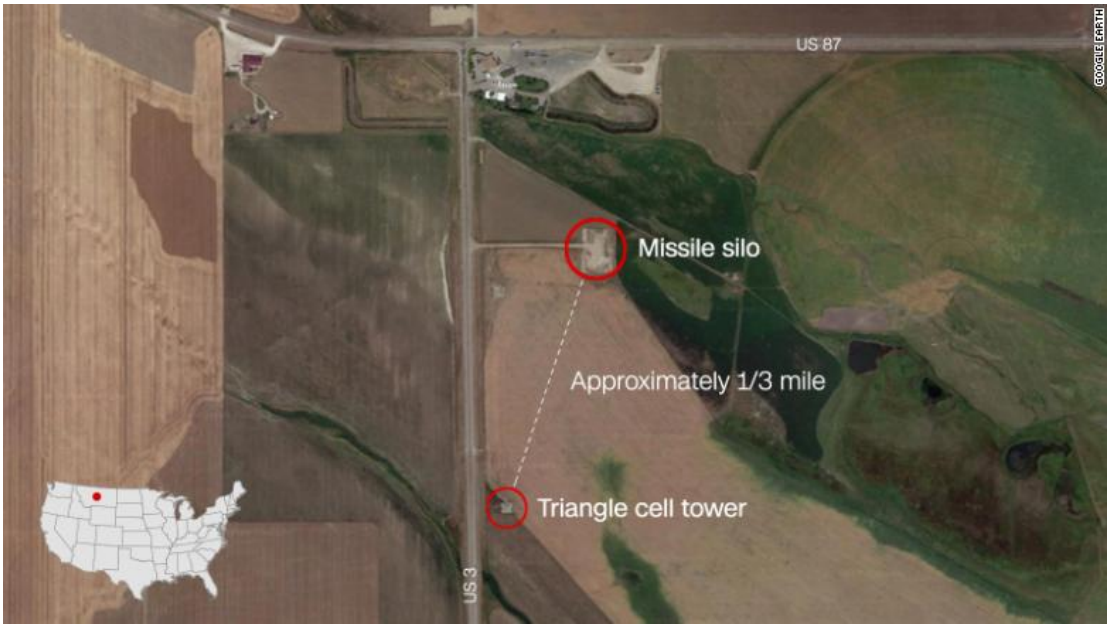
A Triangle Communication cell phone tower in rural Montana, less than half a mile from a fenced-in ICBM silo

Rural Wireless

Across the US there are vast, rural expanses where signals from the country's major wireless carriers do not reach. In their place residents and visitors rely on smaller independent carriers.

Those federal dollars used to subsidize those carriers come out of the multi-billion dollar Universal Services Fund, which helps fund wireless and broadband connectivity to poor and rural communities. Last year, FCC chairman Ajit Pai proposed a rule that would prohibit carriers from using USF funds to buy equipment from Huawei and other companies deemed to be national security threats.

The company operating the towers among the Montana missile fields is called Triangle Communication Systems. Their FCC filings make clear that part of their towers' radio network is manufactured by Huawei. At least five cell phone towers operated by Triangle in Montana are less than three miles from ICBM silos as well as, in at least one case, a launch control center, according to the FCC filings and data from the Federation of American Scientists (FAS).



Triangle Communication Systems network is in part equipped by Huawei, according to engineering documents submitted to FCC. Their towers are partially scattered among missile fields

More than 600 miles to the south, the F.E. Warren Air Force Base oversees ICBM fields that cover parts of Wyoming, Nebraska, and Colorado. In southeastern Wyoming, portions of the silo field are covered by a carrier called Union Wireless. The company operates two sites around the 12,000-square mile silo field in addition to at least 53 other towers across

Wyoming. At least one of those sites is less than six miles from two missile silos, according to FCC filings and FAS data.

In a public statement to the FCC last June, Union's Chief Technical and Operations Officer Eric Woody said that Huawei manufactures "approximately 75%" of Union's equipment. It's unclear whether Huawei gear is used at Union towers that are close to the silos.

Neither Triangle nor Union responded to requests for comment. Both companies are members of the Rural Wireless Association, a trade group of small wireless carriers with fewer than 100,000 subscribers each. A quarter of RWA's roughly 60 member companies use Chinese technology, the groups says. A Huawei official, US vice president of sales William Levy, sits on the RWA board of directors.

RWA says there has been no direction from the Pentagon over how to mitigate any risk posed by the carriers' Chinese technology. Nor has there been any offer to help replace the gear, which is up to 40 percent cheaper and could cost as much as $1 billion to switch out, the group says.

"My members are concerned and they want to do the right thing. So, to the extent that there's information that could be shared with them they'd like to do what's right," RWA's general counsel Carri Bennet told CNN. "Ripping the equipment out from their perspective isn't really going to be in the cards because these networks will not be functional."

"If anyone pointed out to them that this is harmful, they would comply, they would get rid of it," she continued. "They would hope the government wouldn't throw the baby out with the bathwater and try to come up with something to fix it."

A spokesman for STRATCOM declined to go into detail about its relationship with the rural carriers, or what precautionary measures are taken, saying only: "As a part of our force posture, we maintain a concerned awareness of activities within proximity of our installations and sites."

The Department of Defense would not clarify its relationship or what if any conversations it has had with rural carriers around the issue of Huawei. Acting Secretary of Defense Patrick Shanahan told CNN in a statement that the Pentagon "is working closely with our industrial and research partners to develop comprehensive and innovative solutions for both the Department and commercial industries. The United States and our allies and partners must demand nothing less than robust, trusted, and secure next-generation communications systems."

The issue over Chinese technology being deployed near military installations has come up before. In 2012, the Obama administration blocked a Chinese company, Sany Group, from building a wind farm near a naval facility in Oregon out of concerns for national security. At the time, President Barack Obama said there was "credible evidence" that the Chinese group "might take action that threatens to impair the national security of the United States."

Said Lewis, "The Pentagon knows that using Huawei creates risk. And they are struggling over how best to deal with that."