5G Wireless Technology Raises Security Fears

As more devices are connected, the potential dangers expand

With 5G, the telecom system itself may create an ever-larger target for bad actors.

By *John D. McKinnon* Sept. 12, 2018 10:04 p.m. ET

WASHINGTON—By now, the potential benefits of next-generation 5G wireless are well known, such as huge new networks of connected devices, and nifty autonomous vehicles.

Less understood are the security risks—from huge new networks of connected devices, and nifty autonomous vehicles.

The fact is that almost every advance in 5G comes with a new set of security worries. Perhaps the biggest concern is the expected flood of connected household devices, many of which already have been hacked and used in denial-of-service attacks, like one in late 2016 that made major services such as Netflix and Twitter unreachable for a day.

With 5G, the telecommunications system itself will become so central to everyday life that experts fear it will create an ever-larger target for malicious actors. There also are worries that 5G will make it easier for hackers to turn autonomous vehicles, medical procedures and implantable devices into lethal weapons.

As 5G facilitates a vast expansion of devices and networks, “these start to become large targets, and ripe for attack,” says Bruce Potter, chief information security officer at Expel Inc., a cybersecurity startup in Herndon, Va. “We have a fairly large problem ahead to figure out how to secure all the components” of 5G, he adds.

The China threat

U.S. vulnerability could grow even more if domestic companies lose the race with companies abroad to dominate 5G technology. And that is particularly true if the industry comes to rely on Chinese equipment, many U.S. policy makers say.

“Building and designing a telecom network gives you an intelligence advantage,” says James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, a think tank. “If you’re going to burgle a house…it’s easier to burgle” if you built it, he says.

Many U.S. officials say their approach to securing the 5G future is working so far. “It’s a challenge, no way around it, but it’s something everyone I’ve talked to is taking seriously,” says Brendan Carr, a Republican member of the Federal Communications Commission. “We’re bringing all the right people and agencies to bear, so we’re in good shape in that sense.”

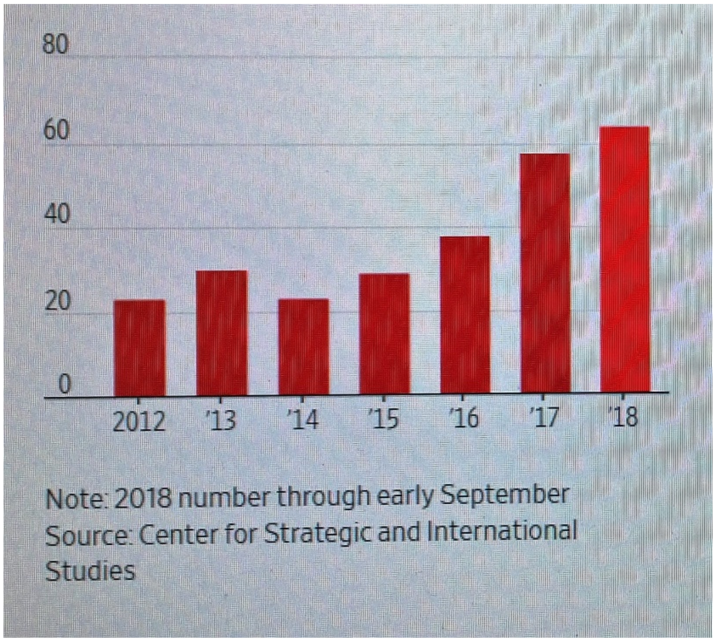
Not everyone agrees, though. Democratic FCC Commissioner Jessica Rosenworcel, for one, has chided the agency for moving slowly on providing the airwaves that 5G will demand. That could mean the U.S. is falling behind in the race to dominate 5G technology. Moreover, the U.S. government’s response so far to cybersecurity—and 5G security in particular—has been criticized as haphazard, because of confusing lines of authority.

DHS limits

The government’s lead agency for many cybersecurity issues, the Department of Homeland Security, acknowledges it doesn’t have the authority to prevent some types of problems.

Growing Target

Cybersecurity attacks could accelerate with5G technology, which will connect far more devices than today’s networks. The number of cyber incidents with losses of more than $1million:



Note: 2018 number through early September
Source: Center for Strategic and International Studies

“DHS is not a regulatory agency, and our authority to prohibit use of software only applies to Federal civilian executive-branch departments and agencies,” an agency official says.

A few White House advisers on the National Security Council earlier this year recommendedwhat amounts to a nationalized 5G system, according to a leaked version of their report. But telecommunications firms and lawmakers of both parties roundly criticized the idea, and its main proponent, an Air Force general, is no longer assigned to the NSC.
Now the government is stepping up efforts to work with business to plug vulnerabilities.

“I don’t want to stifle innovation, and 5G is going to encourage all types of innovation, so we continue to work with industries to make sure we’re building security in,” says Rep. Jim Langevin (D., R.I.), a founder of the House Cybersecurity Caucus.

For example, federal officials are working with many device makers—including household and medical device makers—to make it easier to head off attacks.

In addition, the U.S. Congress recently passed legislation that bars government agencies and contractors from using telecommunications equipment made by Huawei Technologies Co. and ZTE Corp. , leaders in China’s 5G effort. The move expands on previous restrictions that Congress has adopted since concerns began to be raised about the firms’ equipment around 2012. The worry was that Huawei and ZTE were building back doors into their network equipment that the Chinese government could tap into.

A spokesman for Huawei, which denies such accusations, says that restricting the purchase of its equipment in the U.S. “actually does nothing to enhance the real national security of the U.S. It does nothing to identify real security risks or protect the security of the global technology supply chain.”

ZTE didn’t respond to requests for comment.

Major carriers have already stopped using the Chinese companies’ network equipment. But there are fears among security experts that China eventually could gain so much power in the market for 5G network equipment that U.S. companies would have no choice but to use Chinese equipment.

Software rules

Hardware is expected to be less critical to future networks, as software does more of the work, a shift that will boost security in many respects, experts say. Software-defined networks, or SDNs, make security much more flexible and resilient, according to industry experts. For instance, if there’s a breach, it can be contained fairly quickly to a small area.

But there are always trade-offs. As software becomes more important, defects and bugs in the coding can provide great points of entry and tools for attackers, according to some experts.

Some lawmakers, meanwhile, say more dramatic steps might be necessary soon. A number are discussing incentives such as legislation that would give businesses, including telecom firms, legal protection from lawsuits provided they build in sufficient cybersecurity measures.

Mr. McKinnon is a reporter in The Wall Street Journal’s Washington bureau. He can be reached at john.mckinnon@wsj.com.

Appeared in the September 13, 2018, print edition as 'More Connections, More Concerns.'