

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/the-good-news-about-5g-security-11573396200>

JOURNAL REPORTS: TECHNOLOGY

The Good News About 5G Security

We know about the supply-chain risks that could make 5G vulnerable to spying. But there's another side to this.

By Adam Janofsky

Nov. 10, 2019 9:30 am ET

Lost amid recent security concerns about Chinese suppliers of next-generation wireless networks, there is a bigger, more positive story: 5G will provide big benefits when it comes to protecting sensitive data.

The Trump administration in recent months has warned about supply-chain risks that could make these networks vulnerable to spying or disruptive attacks, and has tried to pressure U.S. allies from using equipment manufactured by Chinese telecom giant Huawei Technologies Co. Those concerns are valid, cybersecurity experts say.

JOURNAL REPORT

- • [Read more at WSJ.com/5Greport](https://www.wsj.com/5Greport)

MORE IN 5G TECHNOLOGY

- • [Squabbling Trips Up U.S. in 5G Race](#)
 - • [5G Plus AI Can Transform Industries](#)
 - • [Personal Privacy in the 5G Age](#)
 - • [Life Without Broadband](#)
-

But they also say that 5G—which is expected to be 100 times faster than 4G networks and could enable new technologies such as self-driving cars and remote surgery—will have new features that will make it easier for companies to identify cyber threats, authenticate users and segment their networks to prevent an attack from quickly spreading throughout an organization.

“5G will be more secure than the platform we have today,” says Chandra McMahon, chief information security officer for Verizon Communications Inc. “Security is designed into 5G and there will be additional [security] technical features.”

Network slicing

One of these features is network slicing, a network architecture that enables multiple, isolated virtual networks on the same physical infrastructure. This type of design reduces ease of access to the network as a whole and allows organizations to apply specific security tools and policies to different slices. Slicing can also be a boon for privacy, because information related to each segment isn't shared among the other slices.

For example, one network slice can be allotted to a health-care provider's connected medical devices. Such devices collect sensitive patient data and could cause health and privacy risks if compromised by cybercriminals. A separate slice could be used for less critical functions, such as maintaining the hospital's website.

Cyberattacks affect only the slice being targeted and are therefore easier to contain, says Lenovo Group Ltd. Chief Information Security Officer Jason Ruger. "If there's a distributed denial-of-service attack or a computer worm affecting one slice of the network, the other slices aren't exposed," he says.

Spotting threats

Another potential security benefit of 5G is its effect on artificial-intelligence tools, which companies increasingly use to solve cybersecurity challenges.

Perhaps the biggest boost from 5G for AI technology will be enhancing the speed and volume of data that can flow through an organization's network. With 5G, corporate security operations centers can gather and analyze a huge amount of information collected by sensors and other Internet of Things devices that are expected to proliferate over the next few years.

This will make it easier for companies to, for example, spot suspicious activity such as a hacker trying to access parts of the network that aren't typically visited, or attempting to download an unusually large amount of data. AI-enabled tools could also help security teams quickly and automatically detect malware when an employee clicks on a suspicious document by analyzing characteristics including the file's size and how the code is distributed in it.

Authentication, trust

Another valuable security feature of 5G can be making communication more trustworthy, says Doug Brake, director of broadband and spectrum policy at the Information Technology and Innovation Foundation, a think tank in Washington, D.C. The high-frequency radio waves used by 5G are more directional than those used by 4G, which allows them to transmit large amounts of data without interfering with other wireless signals.

Those properties also make the data harder to intercept, Mr. Brake says. "You can be confident that your signal is going where it's going and no one is listening in."

Another plus for security is that the waves used by 5G will require a new type of infrastructure that could lead to stronger, location-based authentication, says Lenovo's Mr. Ruger. Because the waves have trouble traveling long distances, 5G networks will augment traditional cellular towers with smaller antennas about 1,000 feet apart on buildings, telephone poles and other structures.

"You would know if someone is within a couple-block radius of their house when they're logging in," for example, which makes it easier to spot impostors, Mr. Ruger says.

Challenges ahead

Although 5G brings several cybersecurity benefits to organizations, there are many new risks as well. To start with, the expected explosion of internet-connected devices will bring with it a vastly expanded field of potential targets for hackers. Regulators and industry groups need to develop stronger rules, expectations and mandated cooperation to face such challenges, says Tom Wheeler, former chairman of the Federal Communications Commission under President Barack Obama. Telecommunications firms have been developing cybersecurity standards for 5G, but regulators and other government agencies have had limited involvement in the process, Mr. Wheeler says.

"There needs to be some kind of independent oversight....Wouldn't it be great to have cybersecurity as a forethought, rather than an afterthought?" he says. "We shouldn't be blinded by the promise of what's to come."

Some industry experts remain cautious in their appraisal of 5G's promises. When 5G rolls out broadly, some cybersecurity risks and vulnerabilities will likely remain unaddressed, says John Villasenor, a professor of engineering, public policy, law and management at the University of California, Los Angeles. To him, the big question will be how much damage those risks can cause.

"I'm not very confident that we're going to be on top of these problems," Prof. Villasenor says. "People only get cybersecurity right after they get it wrong. We're going to learn the hard way, and hopefully the mistakes will not be particularly costly and harmful."

Mr. Janofsky is a former Wall Street Journal reporter. He can be reached at reports@wsj.com.

-
- **College Rankings**
 - **College Rankings Highlights**

- **Energy**
- **Funds/ETFs**
- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.