

5G presents security challenge for telecom operators

February 28 2019, by Erwan Lucas



Uses for the lightning-fast 5G network will be virtually limitless and include autonomous cars

While Washington's concerns that future 5G wireless networks could be vulnerable to spying by China have dominated headlines, businesses have long been pushing to make sure the technology is as secure as possible.

With fifth-generation wireless networks, or 5G, starting to be rolled out this year, the issue of 5G security was in focus at the Mobile World Congress trade fair which got under way Monday in Barcelona.

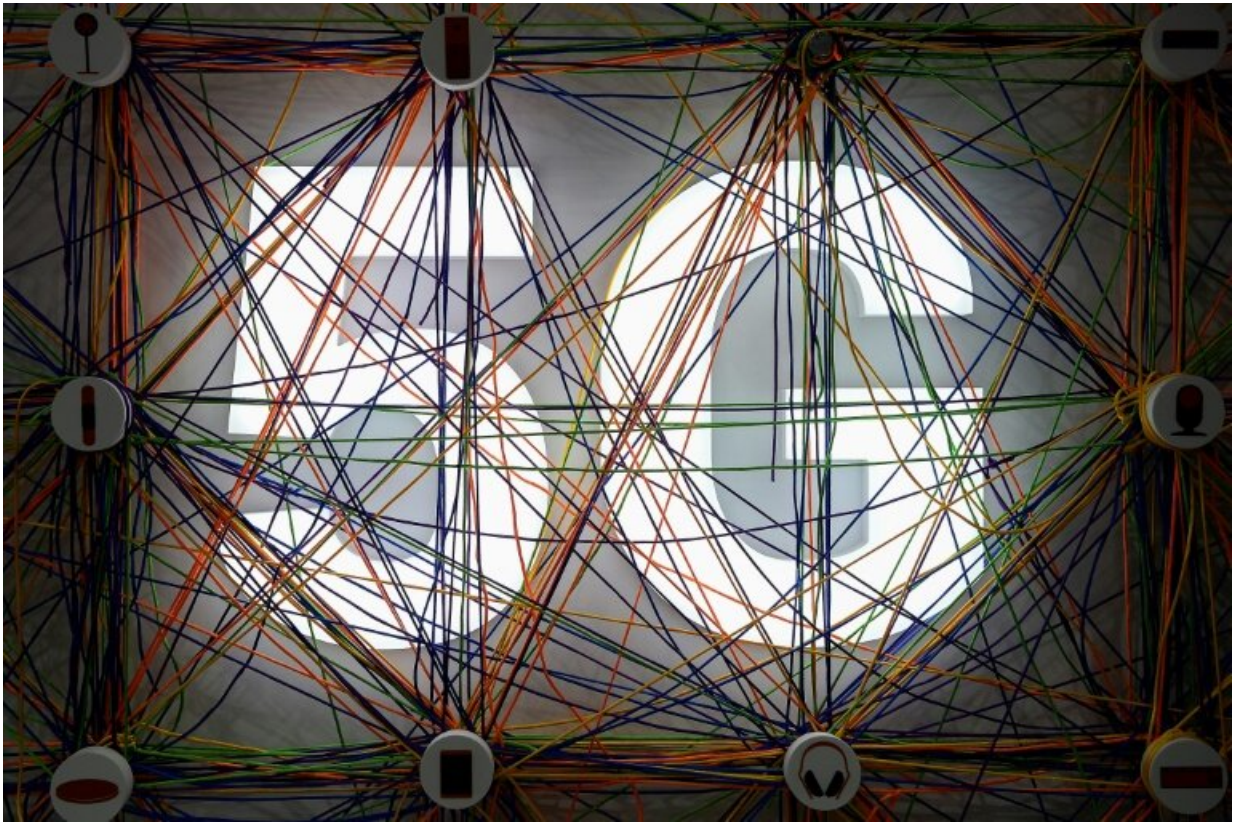
Unlike upgrades of wireless networks in the past, 5G will deliver not just faster phone and [computer data](#) but also help connect up cars, appliances, cargo and crop equipment.

Washington has warned that allowing Chinese firms like Huawei to provide the equipment to build 5G networks could leave them vulnerable to spying on the part of China but this is only one of the risks.

5G's much faster speeds, vast data capacity and lower latency—or [response time](#)—are expected to underpin entirely new technologies such as self-driving cars and telemedicine—which in turn may attract cyberintrusions by criminals or terrorists.

"There will be more data which will be transferred...it is clear that security is much more complicated," said Yannick Sadowy, the director for telecoms and media at consulting firm Accenture.

Mathieu Lagrange, who is responsible for internet security at com institute, said the risks to 5G's security "were taken into account" when the norms for the technology were established.



5G may just to be too complex to protect it from all attempts at interference

But a study by the University of Lorraine in France found that the new wireless network still contains some security holes which were already present in previous networks, 3G and 4G.

5G offers "improved data protection when compared to the previous wireless norms" but "flaws persist and the weaknesses that have been identified" could allow "several cyberattacks and have an impact on the protection of privacy," it said.

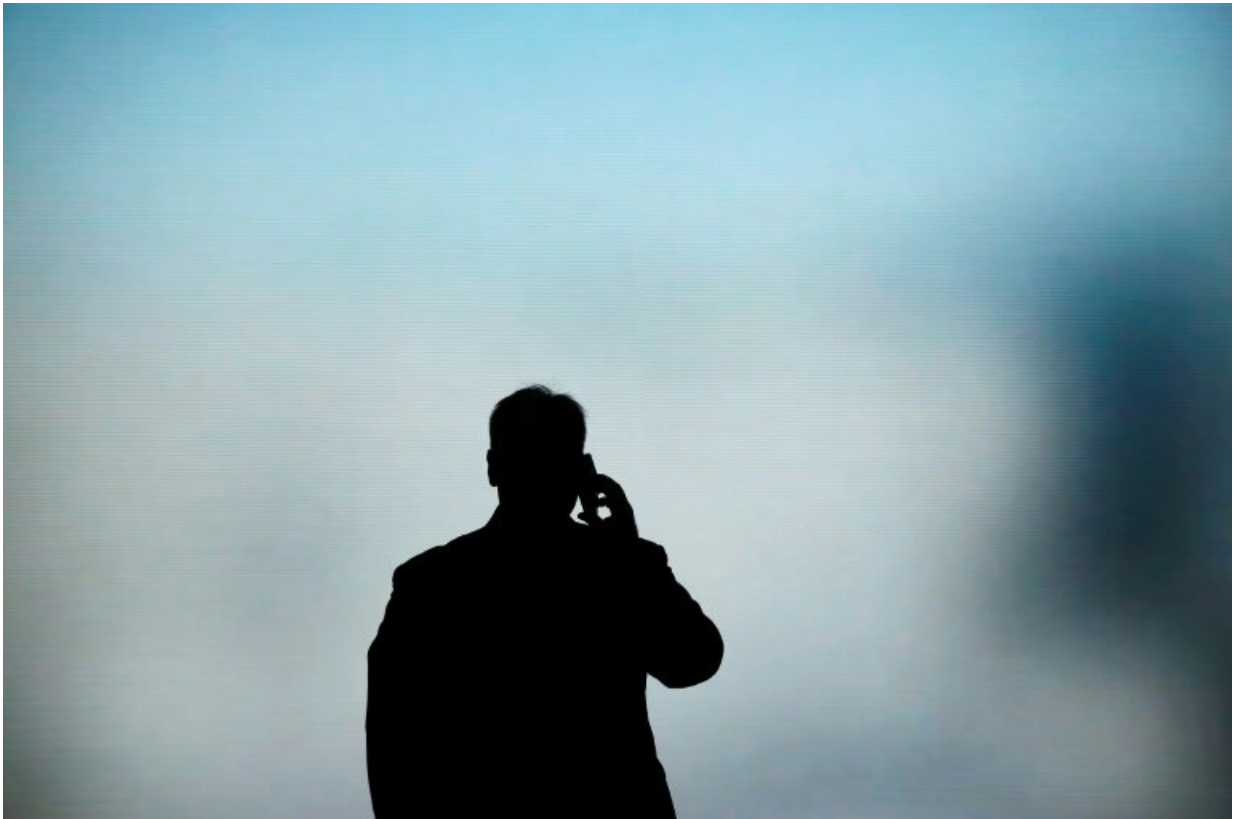
Experts say the architecture of 5G networks also presents entirely new security challenges.

Fifth generation wireless networks use "network virtualisation", which refers to moving some resources which have traditionally been delivered in physical hardware to a virtual software-based network.

It is designed to allow the network to make better use of data transfer rates and provide more flexibility to 5G networks.

"Operators are moving from a hardware system to a virtualised and fully automated one," said Darren Anstee, technology director at Netscout, which provides software for networks.

"Security is about visibility, when you can't see everything on your network, this is when you have a problem," he added.



"Nothing will ever be 100 percent secure"

Nothing 100% secure

5G allows for the available bandwidth to be split up into channels, each of which is independent from others and can be separately secured, which some experts say can help boost security.

"We can create a kind of micro-networks, with different levels of security. The idea is to compartmentalise the network according to different uses," said Laurent Boutet, a [systems engineer](#) at US computer networking company F5Network.

Mobile communications industry body GSMA, which stages the Mobile World Congress, estimates the number of connected devices will triple to 25 billion by 2025.

For Dexter Thillien, an analysts at Fitch Solutions, the main challenge for security is this rise in the "number of entry points, considering the exponential number of objects which will be connected."

"From the point of view of [security](#), the [network](#) itself is secondary," he said.

"You have to keep in mind that nothing will ever be 100 percent secure. We still don't have a precise idea of how billions or even trillions of connected objects could affect networks, it is still unknown at this point," said Thillien.

© 2019 AFP

Citation: 5G presents security challenge for telecom operators (2019, February 28) retrieved 3 May 2024 from <https://phys.org/news/2019-02-5g-telecom.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.