Opinion

If 5G Is So Important, Why Isn’t It Secure?

The network must be secure enough for the innovations it promises.

By Tom Wheeler

Mr. Wheeler is a former chairman of the Federal Communications Commission.

Jan. 21, 2019

The Trump administration’s so-called “race” with China to build new fifth-generation (5G) wireless networks is speeding toward a network vulnerable to Chinese (and other) cyberattacks. So far, the Trump administration has focused on blocking Chinese companies from being a part of the network, but these efforts are far from sufficient. We cannot allow the hype about 5G to overshadow the absolute necessity that it be secure.

Our current wireless networks are fourth-generation, or 4G. It was 4G that gave us the smartphone. Reaching the next level of mobile services, however, requires increased speed on the network. Fifth-generation networks are designed to be 10 to 100 times faster than today’s typical wireless connection with much lower latency (response time). These speeds will open up all kinds of new functional possibilities. Those new functions, in turn, will attract cyberintrusionsjust like honey attracts a bear.

Some envision 5G as a kind of “wireless fiber” for the delivery of television and internet much like a cable system does today. Iranians hacking the delivery of “Game of Thrones” isn’t good, but the real transformational promise of 5G goes far beyond wireless cable and its security is much more critical.

The most exciting part of the 5G future is how its speed will change the very nature of the internet. Thus far, the internet has been all about transporting data from point A to point B. Today’s internet-connected car may be able to get driving directions sent to it, but it is essentially the same as getting email: the one-way transportation of pre-existing information. The autonomous car is something vastly different, in which the 5G network allows computers to orchestrate a flood of information from multitudes of input sensors for real time, on-the-fly decision-making. It is estimated that the data output of a single autonomous vehicle in one day will be equal to today's daily data output of three thousand people.

Leadership in 5G technology is not just about building a network, but also about whether that network will be secure enough for the innovations it promises. And the 5G "race" is more complex and dangerous than industry and the Trump administration portray. When 5G enables autonomous vehicles, do we want those cars and trucks crashing into each other because the Russians hacked the network? If 5G will be the backbone of breakthroughs such as remote surgery, should that network be vulnerable to the North Koreans breaking into a surgical procedure? Innovators, investors and users need confidence in the network's cybersecurity if its much-heralded promise is to be realized.

"It is imperative that America be first in fifth-generation (5G) wireless technologies," President Trump wrote in an October Presidential Memorandum of instructions to federal agencies. While the administration, especially the Trump Federal Communications Commission (F.C.C.), makes much of how the 5G "race" with China is a matter of national security, not enough effort is being put into the security of the network itself. Nowhere in the president's directive, for instance, was there a word about protecting the cybersecurity of the new network.

As the President's National Security Telecommunications Advisory Committee told him in November, "the cybersecurity threat now poses an existential threat to the future of the Nation." Last January, the brightest technical minds in the intelligence community, working with the White House National Security Council (N.S.C.), warned of the 5G cybersecurity threat. When the proposed solutions included security through a federally-owned network backbone, the wireless industry screamed in protest. The chairman of the Trump F.C.C. quickly echoed the industry line that "the market, not government, is best positioned to drive innovation and leadership." Government ownership may not be practicable, but the concerns in the N.S.C. report have been dismissed too readily.

Worse than ignoring the warnings, the Trump administration has repealed existing protections. Shortly after taking office, the Trump F.C.C. removed a requirement imposed by the Obama F.C.C. that the 5G technical standard must be designed from the outset to withstand cyberattacks. For the first time in history, cybersecurity was being required as a forethought in the design of a new network standard — until the Trump F.C.C. repealed it. The Trump F.C.C. also canceled a formal inquiry seeking input from the country's best technical minds about 5G security, retracted an Obama-era F.C.C. white paper about reducing cyberthreats, and questioned whether the agency had any responsibility for the cybersecurity of the networks they are entrusted with overseeing.

The simple fact is that our wireless networks are not as secure as they could be because they weren't designed to withstand the kinds of cyberattacks that are now common. This isn't the fault of the companies that built the networks, but a reflection that when the standards for the current fourth-generation (4G) technology were set years ago, cyberattacks were not a front-and-center concern.

The Trump administration has been told that cybersecurity is an "existential risk." The new Congress should use its oversight power to explore just why the administration has failed to protect against that risk, especially when it comes to the next generation of networks.

Tom Wheeler, the chairman of the Federal Communications Commission from 2013 to 2017, is a visiting fellow at the Brookings Institution and a fellow at the Harvard Kennedy School. His new book, "From Gutenberg to Google: The History of Our Future," will be published in February.

Follow The New York Times Opinion section on Facebook, Twitter (@NYTopinion) and Instagram.