THE NEW YORKER

THE TERRIFYING POTENTIAL OF THE 5G NETWORK

The future of wireless technology holds the promise of total connectivity. But it will also be especially susceptible to cyberattacks and surveillance.

By Sue Halpern

April 26, 2019

In January, 2018, Robert Spalding, the senior director for strategic planning at the National Security Council, was in his office at the Eisenhower Executive Office Building, across the street from the White House, when he saw a breaking-news alert on the Axios Web site. “Scoop,” the headline read, “Trump Team Considers Nationalizing 5G Network.” At the time, Spalding, a brigadier general in the Air Force who previously served as a defense attaché in Beijing, had been in the military for nearly three decades. At the N.S.C., he was studying ways to insure that the next generation of Internet connectivity, what is commonly referred to as 5G, can be made secure from cyberattacks. "I wasn't looking at this from a policy perspective," he said. "It was about the physics, about what was possible." To Spalding's surprise, the Axios story was based on a leaked early draft of a report he'd been working on for the better part of a year.

Two words explain the difference between our current wireless networks and 5G: speed and latency. 5G—if you believe the hype—is expected to be up to a hundred times faster. (A two-hour movie could be downloaded in less than four seconds.) That speed will reduce, and possibly eliminate, the delay—the latency—between instructing a computer to perform a command and its execution. This, again, if you believe the hype, will lead to a whole new Internet of Things, where everything from toasters to dog collars to dialysis pumps to running shoes will be connected. Remote robotic surgery will be routine, the military will develop hypersonic weapons, and autonomous vehicles will cruise safely along smart highways. The claims are extravagant, and the stakes are high. One estimate projects that 5G will pump twelve trillion dollars into the global economy by 2035, and add twenty-two million new jobs in the United States alone. This 5G world, we are told, will usher in a fourth industrial revolution.

A totally connected world will also be especially susceptible to cyberattacks. Even before the introduction of 5G networks, hackers have breached the control center of a municipal dam system, stopped an Internet-connected car as it travelled down an interstate, and sabotaged home appliances. Ransomware, malware, crypto-jacking, identity theft, and data breaches have become so common that more Americans are afraid of cybercrime than they are of becoming a victim of violent crime. Adding more devices to the online universe is destined to create more opportunities for disruption. "5G is not just for refrigerators," Spalding said. "It's farm implements, it's airplanes, it's all kinds of different things that can actually kill people or that allow someone to reach into the network and direct those things to do what they want them to do. It's a completely different threat that we've never experienced before."

Spalding's solution, he told me, was to build the 5G network from scratch, incorporating cyber defenses into its design. Because this would be a massive undertaking, he initially suggested that one option would be for the federal government to pay for it and, essentially, rent it out to the telecom companies. But he had scrapped that idea. A later draft, he said, proposed that the major telecom companies—Verizon, A.T. & T., Sprint, and T-Mobile—form a separate company to build the network together and share it. "It was meant to be a nationwide network," Spalding told me, not a nationalized one. "They could build this network and then sell bandwidth to their retail customers. That was one idea, but it was never that the government would own the network. It was always about, How do we get industry to actually secure the system?"

Even before Spalding began working on his report, the telecom companies were rolling out what they were calling their new 5G services in test markets around the country. In 2017, Verizon announced that it would be introducing 5G in eleven municipalities, including Dallas, Ann Arbor, Miami, and Denver. A.T. & T. was testing its service in a dozen cities. T-Mobile was concentrating on Spokane. For the most part, they were building their new services on top of existing infrastructure—and inheriting its vulnerabilities. As the Clemson University professor Thomas Hazlett told me, "This is just the transitional part. You have various experiments, you do trial in the market, and various deployments take place that lay a pathway to something that will be truly distinguishable from the old systems."

In the meantime, the carriers jockeyed for position. A lawsuit brought by Sprint and T-Mobile, which was settled on Monday, claimed that A.T. & T.'s 5GE service, where "E" stands for "evolution," was just 4G by another name. According to Spalding, when the carriers heard that the government was considering “nationalizing” the future of their industry, they quickly mobilized against it. “As I’ve talked to people subsequently, they said they’ve never seen that industry unite so quickly,” Spalding said. “They have such support in government and on the Hill and in the bureaucracy, and they have such a huge lobbying contingent, that it was across the board and swift.” The Axios story came out on a Sunday. The following day, Ajit Pai, the chairman of the Federal Communications Commission, roundly rejected any idea of federalizing the Internet, saying that “the market, not government, is best positioned to drive innovation and investment.” By Wednesday, Spalding was out of a job. “There was no ‘Hey, thank you for your service,’ ” Spalding told me. “It was just ‘Get out. Don’t let the door hit your butt.’ ”

Huawei, a Chinese manufacturer of consumer electronics and telecommunications equipment, is currently the global leader in 5G technology. Founded, in the eighties, by Ren Zhengfei, an engineer who began his career in the People’s Liberation Army, Huawei has been accused by cybersecurity experts and politicians, most notably Donald Trump, of being a conduit to Chinese intelligence. In an op-ed in the Washington *Post*, the Republican senators Tom Cotton, of Arkansas, and John Cornyn, of Texas, characterized the company, which is funded with subsidies from the Chinese government, as a Trojan horse that could “give China effective control of the digital commanding heights.” They tell the story of the African Union, which installed Huawei servers in its headquarters, in Addis Ababa, only to discover that those servers had been sending sensitive data back to China every evening. Although Huawei vigorously denies that it is an agent of the Chinese government, the senators pointed out, the company is subject to a Chinese law that requires companies to coöperate with the state intelligence apparatus. The *Times* of London reported that the C.I.A. has evidence that Huawei has taken money from the P.L.A., as well as from branches of the Chinese intelligence service. Australia, Japan, and New Zealand have joined with the United States in banning Huawei hardware from their networks.

So far, though, the Trump Administration’s campaign to shut out Huawei is finding limited traction. The European Union is poised to reject American entreaties, with individual countries like Portugal and Germany expressing a willingness to use Huawei equipment. Canada is relying on Huawei for at least one 5G trial. Even A.T. & T., which is bound by the federal guidelines that will go into effect next year in the U.S., continues to use Huawei equipment in Mexico, where it is the third-largest wireless company. Huawei equipment is cheaper than its Western rivals and, in the estimation of researchers at the Defensive Innovation Board (DIB), which advises the Secretary of Defense on new technologies, in many cases, it is superior. By the start of this year, Huawei had cornered nearly thirty per cent of the global telecommunications-equipment market, and its revenue was thirty-nine-per-cent higher than the year before. According to the DIB, its continued growth “will allow China to promote its preferred standards and specifications for 5G networks and will shape the global 5G product market going forward.”

There are very good reasons to keep a company that appears to be beholden to a government with a documented history of industrial cyber espionage, international data theft, and domestic spying out of global digital networks. But banning Huawei hardware will not secure those networks. Even in the absence of Huawei equipment, systems still may rely on software developed in China, and software can be reprogrammed remotely by malicious actors. And every device connected to the fifth-generation Internet will likely remain susceptible to hacking. According to James Baker, the former F.B.I. general counsel who runs the national-security program at the R Street Institute, “There’s a concern that those devices that are connected to the 5G network are not going to be very secure from a cyber perspective. That presents a huge vulnerability for the system, because those devices can be turned into bots, for example, and you can have a massive botnet that can be used to attack different parts of the network."

This past January, Tom Wheeler, who was the F.C.C. chairman during the Obama Administration, published an Op-Ed in the New York *Times* titled "If 5G Is So Important, Why Isn't It Secure?" The Trump Administration had walked away from security efforts begun during Wheeler's tenure at the F.C.C.; most notably, in recent negotiations over international standards, the U.S. eliminated a requirement that the technical specifications of 5G include cyber defense. "For the first time in history," Wheeler wrote, "cybersecurity was being required as a forethought in the design of a new network standard—until the Trump F.C.C. repealed it." The agency also rejected the notion that companies building and running American digital networks were responsible for overseeing their security. This might have been expected, but the current F.C.C. does not consider cybersecurity to be a part of its domain, either. "I certainly did when we were in office," Wheeler told me. "But the Republicans who were on the commission at that point in time, and are still there, one being the chairman, opposed those activities as being overly regulatory."

The Trump Administration, keen to win what it has characterized as "the race to 5G," may be more interested in attempting to put a brake on Huawei's—and, by extension, China's—progress. In January, the company's chief financial officer, Meng Wanzhou, a daughter of the Huawei founder, was indicted on thirteen counts in the U.S., including breaking sanctions against Iran, money laundering, and obstruction of justice. Meng is currently under arrest in Canada and fighting extradition. Ajit Pai, the F.C.C. chairman, recently announced that the commission will block another Chinese company, China Mobile, from operating in the U.S., again citing security concerns. "If we didn't have these other trade issues with China, it would be easier to just accept the [Administration's] security statements as truth," Scott Wallsten, an economist and the president of the Technology Policy Institute, told me.

"But when it gets mixed up with all these other trade issues, it makes it a little more suspect."

In October, Trump signed a memorandum on "Developing a Sustainable Spectrum Strategy for America's Future." A few weeks later, the F.C.C. auctioned off new swaths of the electromagnetic radio spectrum. (There was another auction last month, with more scheduled for later this year.) Opening up new spectrum is crucial to achieving the super-fast speeds promised by 5G. Most American carriers are planning to migrate their services to a higher part of the spectrum, where the bands are big and broad and allow for colossal rivers of data to flow through them. (Some carriers are also working with lower-spectrum frequencies, where the speeds will not be as fast but likely more reliable.) Until recently, these high-frequency bands, which are called millimetre waves, were not available for Internet transmission, but advances in antenna technology have made it possible, at least in theory. In practice, millimetre waves are finicky: they can only travel short distances—about a thousand feet—and are impeded by walls, foliage, human bodies, and, apparently, rain.

To accommodate these limitations, 5G cellular relays will have to be installed inside buildings and on every city block, at least. Cell relays mounted on thirteen million utility poles, for example, will deliver 5G speeds to just over half of the American population, and cost around four hundred billion dollars to install. Rural communities will be out of luck—too many trees, too few people—despite the F.C.C.'s recently announced Rural Digital Opportunity Fund. According to Blair Levin, a communications analyst and former F.C.C. chief of staff in the Clinton Administration, the fund "has nothing to do with 5G." Rather, it will subsidize companies to lay fibre-optic cable that, minimally, will provide speeds forty times slower than what 5G promises.

Deploying millions of wireless relays so close to one another and, therefore, to our bodies has elicited its own concerns. Two years ago, a hundred and eighty scientists and doctors from thirty-six countries appealed to the European Union for a moratorium on 5G adoption until the effects of the expected increase in low-level radiation were studied. In February, Senator Richard Blumenthal, a Democrat from Connecticut, took both the F.C.C. and F.D.A. to task for pushing ahead with 5G without assessing its health risks. “We’re kind of flying blind here,” he concluded. A system built on millions of cell relays, antennas, and sensors also offers previously unthinkable surveillance potential. Telecom companies already sell location data to marketers, and law enforcement has used similar data to track protesters. 5G will catalogue exactly where someone has come from, where they are going, and what they are doing. “To give one made-up example,” Steve Bellovin, a computer-science professor at Columbia University, told the *Wall Street Journal*, “might a pollution sensor detect cigarette smoke or vaping, while a Bluetooth receiver picks up the identities of nearby phones? Insurance companies might be interested.” Paired with facial recognition and artificial intelligence, the data streams and location capabilities of 5G will make anonymity a historical artifact.

In China, which has installed three hundred and fifty thousand 5G relays—about ten times more than the United States—enhanced geolocation, coupled with an expansive network of surveillance cameras, each equipped with facial-recognition technology, has enabled authorities to track and subordinate the country’s eleven million Uighur Muslims. According to the *Times*, “the practice makes China a pioneer in applying next-generation technology to watch its people, potentially ushering in a new era of automated racism.”

The United States is not there yet, and may never be. But, as 5G begins to be rolled out, the pressure to capture and capitalize on new streams of data from individuals, businesses, and government will only grow more intense. Building safeguards into the system seems like an obvious and necessary goal. Spalding is now a senior fellow at the Hudson Institute and also advises corporations and other agencies on the cybersecurity threats posed by China. But, he warns, the danger is not limited to a single nation-state. “What is existential to democracy is allowing totalitarian regimes—or any government—full knowledge of everything you do at all times," he said. "Because the tendency is always going to be to want to regulate how you think, how you act, what you do. The problem is that most people don't think very hard about what that world would look like."

A previous version of this post misidentified one of the Chinese companies blocked from operating in the U.S.